



ФАКУЛЬТЕТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сегодня Российская Федерация, как и многие страны мира, является органичной частью глобального информационного общества. В новых условиях ведущую роль в обеспечении устойчивого поступательного развития всех областей общественной жизни играют информационно-телекоммуникационные технологии.

Все мы, хотим того или нет, уже давно находимся на «информационной планете», не имеющей привычных государственных границ в информационном пространстве. На этой планете живут люди всех возрастов, рас, полов, вероисповеданий, использующие новейшие информационные и коммуникационные технологии для личных и общественных целей, во благо и во вред.

В настоящее время угрозы информационной безопасности реализуют не только или не столько хакеры. Соответствующие технологии широко используются в конкурентной борьбе, а также военными организациями и спецслужбами всех стран.

Сложность противодействия угрозам информационной безопасности определяется характером проблемы. Во-первых, угрозы глобальны, они касаются каждого, поскольку все мы имеем дело с информацией. Пока еще около 25 процентов россиян пользуются Интернетом, но это число интенсивно растет. А благодаря реализации ряда национальных проектов пользователем всемирной Сети станет скоро каждый третий житель страны.

Во-вторых, эти угрозы трансграничны, что существенно затрудняет организацию противодействия, поскольку требует объединения усилий различных стран. Ведь жизнь любого социума даже на «информационной планете» невозможна без выработки правил общезначимости.

Глобальная инфраструктура этой жизни завязана на Интернете, возникшем как саморегулируемая система, в которой, прежде всего, применяются технические нормы и правила, позволяющие беспрепятственно устанавливать связи между пользователями, обеспечивать доступ и передачу информации.

Однако Интернет несет обществу и потенциальные угрозы, являющиеся, как водится, обратной стороной его преимуществ:

- отсутствие общепризнанных правил поведения, имеющих обязательную силу, обеспечивающих участникам «сетевых» отношений защиту чести, достоинства, деловой репутации, неприкосновенности частной жизни, общественной нравственности, запрета пропаганды антиобщественного поведения, насилия, в частности, распространения информации о способах совершения террористических актов;

- анонимность присутствия в Сети позволяет распространять ложную информацию, не боясь справедливого наказания; сложность выявления правонарушителя и сбора доказательств затрудняет свершение правосудия;

- отсутствие системы общественного контроля и самоцензуры приводит к тому, что доверие к предоставляемой в Сети информации снижается;

- возможность проникновения в автоматизированные системы, обеспечивающие жизнедеятель-

ность общества, создает угрозу не только нарушения нормальной работы этих систем, но и угрозу жизни людей; (известны случаи удачных попыток проникновения в системы энергоснабжения России и США, в системы, управляющие опасными

производствами, не говоря уже о банковских системах).

Когда речь заходит об обеспечении безопасности любого предприятия, первое, с чего начинается решение этого вопроса, — физическая защита: охранные видеокамеры, датчики, системы сигнализации и контроля доступа приобретаются и устанавливаются в большом количестве. Они непрерывно следят за объектом защиты, анализируют его состояние в заданные моменты или через определенные промежутки времени. Мир физической безопасности понятен любому человеку.

В свою очередь, компьютерная безопасность ориентирована не на физический мир, а на киберпространство, где нарушители — это наборы нулей и единиц, на которые нельзя надеть наручники и которые не могут служить мишенью для лазерного прицела. Информационная система — это тоже своего рода здание, только виртуальное, которое также необходимо защищать от посягательств преступников, но преступников виртуальных, которые действуют на расстоянии и практически безнаказанно проникают в корпоративные сети.

Например, несанкционированный вход в обычное здание блокируется охранником или турникетом. В виртуальном здании для этого используются межсетевые экраны или система аутентификации, которые проверяют входящий в систему (и исходящий из нее) трафик на соответствие различным категориям. Однако злоумышленник для несанкционированного проникновения в здание может подделать пропуск (в виртуальном мире это подделка адреса) или пролезть через окно (в виртуальном мире — через модем). И никакой охранник или турникет не защитит от этого. Аналог механизма охранной сигнализации и оповещения периодически присутствует и в виртуальном мире. Это сканер безопасности, который по требованию администратора безопасности или по расписанию проводит ряд проверок заданных компонентов информационной системы.

Он действует как охранник, периодически обходящий все этажи здания в поисках открытых дверей, незакрытых окон и других лазеек. Только в качестве здания выступает информационная система, а в качестве незакрытых окон и дверей — слабые места в защите этой системы («дыры»).

Получить престижную и востребованную сегодня (а еще больше завтра!) профессию по защите информации от несанкционированного доступа, от

хищения и злонамеренного использования данных, по противодействию легализации (отмыванию) преступных доходов и финансированию терроризма можно на факультете информационной безопасности («Б») НИЯУ МИФИ.

Подготовка кадров ведется по специальности:

- Информационная безопасность автоматизированных систем;
- Информационно-аналитические системы безопасности.

Кафедра «Информационная безопасность банковских систем», заведующий — заместитель Председателя Центрального банка России, д.т.н. М.Ю. Сенаторов.

Завершается процесс автоматизации российских банков. Однако переход к новому «цифровому» бизнесу ставит перед банками многочисленные проблемы, и главная из них — защита информационных ресурсов и, прежде всего, «изнутри».



На факультете сформировался высококлассный профессорско-преподавательский состав; преподавание профильных дисциплин ведется специалистами с «живым» опытом работы на уровне экспертов, руководителей и ведущих сотрудников отечественных и зарубежных фирм и компаний, успешно зарекомендовавших себя на российском рынке информационных технологий. Это «Лаборатория Касперского», «Информзащита», Центр безопасности информации «Маском», ОКБ «Сапр» и ряд других.

В 2004 и 2010 годах факультет стал лауреатом Национальной премии в области информационной безопасности «Серебряный кинжал» «За подготовку специалистов в области информационной безопасности».

Факультет имеет современную лабораторную базу, основу которой составляют: учебно-методический стенд Центрального банка России; учебно-научный комплекс Федеральной службы по техническому и экспортному контролю (ФСТЭК), лаборатории фирм Sun Microsystems, Microsoft, Oracle, Cisco; центр физической защиты.

Издаваемый на факультете научный журнал «Безопасность информационных технологий» (БИТ) в 2007 году награжден Дипломом Всероссийского конкурса электронных СМИ как лучшее профессиональное издание в области информационной безопасности.

На факультете действует специализированный Совет по защите кандидатских и докторских диссертаций.

Постоянно растущий спрос на выпускников факультета как со стороны органов государственного управления, научных и высших учебных заведений страны, так и со стороны банков, финансовых компаний, отечественных и международных организаций и фирм — свидетельство высокого качества подготовки специалистов по защите информации в НИЯУ МИФИ, базовом вузе среди вузов России по данной проблеме.

Если Вы готовы учиться, проявляя настойчивость и инициативу, искать и находить нестандартные решения, если не хотите оказаться «выпускником прошлого», — пожалуйста на факультет «Б». Ждем Вас!

Телефоны: 8 (495) 323-9409, 323-9461, 323-9086.

А.А. Малюк,
декан факультета «Б»,
профессор,
заслуженный работник высшей школы РФ.

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И БЕЗОПАСНОСТЬ



В одной из лабораторий учебно-научного комплекса ФСТЭК на факультете. Идет коллективный поиск не только правильного, но еще и «красивого» решения...

Квалификация — специалист по защите информации и направлению «Информационная безопасность» (бакалавр); профиль — Комплексная защита объектов информатизации (вечернее отделение, контрактная форма обучения — 4 года).

В составе факультета пять специальных и три общеобразовательные кафедры.

Кафедра «Защита информации», заведующий — декан факультета, к.т.н., профессор А.А. Малюк.

По направлению своей учебной деятельности кафедра является базовой и обеспечивает координацию и объединение усилий всех остальных кафедр в рамках общефакультетского проекта по обучению студентов.

Кафедра «Криптология и дискретная математика», заведующий — д.ф.-м.н., профессор, академик РАО Н.Д. Подуфалов.

Кафедра осуществляет углубленную математическую подготовку и обеспечивает изучение основ информатики всеми студентами факультета. Основное же направление деятельности кафедры — обучение студентов владению криптографическими методами защиты информации, которые до недавнего времени были атрибутом государственных структур, обеспечивающих безопасность страны.

Кафедра «Стратегические информационные исследования», заведующий — заместитель генерального директора Службы корпоративной защиты ОАО «Газпром», к.т.н. Ю.Н. Лаврухин.

Кафедра готовит специалистов, способных решать важнейшие задачи по обеспечению национальной безопасности России в информационной сфере, и, прежде всего, в федеральных органах исполнительной власти и на предприятиях оборонного комплекса.

Кафедра «Финансовый мониторинг», заведующий — Ю.А. Чихачин, кандидат экономических наук, заслуженный экономист Российской Федерации, руководитель Федеральной службы по финансовому мониторингу.

Кафедра готовит специалистов по системному анализу и защите информации в финансовой и экономической сферах. Подготовка осуществляется в интересах национальной системы по противодействию легализации (отмыванию) преступных доходов и финансированию терроризма. Специалисты в сфере обеспечения финансовой и экономической безопасности востребованы также в других органах государственной власти и в специализированных подразделениях крупных субъектов финансово-хозяйственной деятельности (банки, страховые и лизинговые компании, организации игорного бизнеса, риэлторские фирмы и т.д.).

Кафедра «Компьютерное право», заведующий — директор Института истории естествознания и техники РАН, космонавт, Герой России, д.ю.н. Ю.М. Батурич.

Основными направлениями деятельности кафедры являются — расследование компьютерных инцидентов, возможное участие в проведении компьютерно-технических экспертиз в соответствии с процессуальным законодательством Российской Федерации.

Состав специальных кафедр логично дополняется кафедрами, образующими «военно-спортивный» комплекс. Это — кафедра военной подготовки, которую возглавляет полковник А.И. Коростелев, и кафедра физического воспитания, во главе которой — профессор, заслуженный мастер спорта, многократный олимпийский чемпион В.И. Старшинов.