МИФИБ

ФАКУЛЬТЕТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И БЕЗОПАСНОСТЬ

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, с удовольствием использующие новейшие информационные и коммуникационные технологии для личных и общественных целей, во благо и во вред.

Неизбежность и целесообразность использования информационных технологий и глобальных коммуникаций влечет за собой неотвратимость угроз информационной безопасности. Каждый из нас, любая фирма, компания, страна, мировое сообщество сталкиваются с этими угрозами и не осознавать это опасно. Потеря информации в личном компьютере в результате проникновения вируса ощутима для его владельца, но нарушение работы систем государственного управления, систем жизнеобеспечения задевает интересы общества, национальные интересы в целом.

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. Можно ожидать, что половина населения почувствует остроту угроз информационной безопасности.

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 общежития.

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 представляемой в Сети информации снижается;***

• ***возможность проникновения в автоматизированные системы, обеспечивающие жизнедеятельность 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.

Использовать для защиты виртуального здания можно те же механизмы физической безопасности, но спроецированные с учетом особенностей информационных технологий. Например, несанкционированный вход в обычное здание блокируется охранником или турникетом. В виртуальном здании для этого используются межсетевой экран 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 периодического действия 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»).

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

Защита информации от несанкционированного доступа, противодействие хищению и злонамеренному использованию данных, хранящихся и обрабатываемых на компьютере, и составляют суть престижной и востребованной сегодня (а еще больше завтра!) профессии, которую можно получить на факультете «Информационная безопасность» («Б») НИЯУ «МИФИ».

Подготовка кадров ведется по специальностям:

• **Комплексное обеспечение информационной безопасности автоматизированных систем (дневное отделение, бюджетная и контрактная формы обучения) – 5 лет.**

• **Комплексная защита объектов информатизации (вечернее отделение, контрактная форма обучения) – 5 лет.**

Квалификация – специалист по защите информации.

В составе факультета пять специальных и две 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. **(kaf42@pisem.net)**.

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 «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»*.

Кафедра «Компьютерное право», заведующий – космонавт, заместитель начальника по научной работе Центра подготовки космонавтов, Герой России, д. ю. н. **Ю.М. Батурин**.

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 – **военная кафедра**, которую возглавляет полковник **Ю.А. Кушнарев**, и **кафедра физического воспитания**, во главе которой – профессор, заслуженный мастер спорта, многократный олимпийский чемпион **В.И. Старшинов**.

Узнать **подробнее о каждой кафедре**, о научных направлениях ее деятельности, о преподавателях, о работе со студентами и аспирантами, можно на сайте факультета – **www.fis.mephi.edu.**

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 году 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», – поступайте на факультет «Б». Ждем Вас!

]Наш сайт: www.fis.mephi.edu.

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

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