



**Дворянкин Сергей Владимирович**,  
декан факультета «Кибернетика,  
информационная безопасность» НИЯУ МИФИ,  
профессор, д.т.н.

## Введение

Такая высокотехнологическая отрасль промышленности, как ядерная энергетика, всегда выступала локомотивом развития самых современных направлений науки и техники, в том числе информационных технологий и обеспечения безопасности. Хотя приоритетной областью деятельности Национального исследовательского ядерного университета «Московский инженерно-физический институт» (НИЯУ МИФИ) является подготовка кадров и проведение научных исследований в интересах атомной отрасли, в университете накоплен значительный опыт выполнения целевых заказов со стороны силовых министерств и ведомств, широко использующих современные достижения науки и техники.

Университет имеет также опыт взаимодействия с организациями МВД России, в частности взаимовыгодного сотрудничества с ВИПК МВД России в части совместной работы по повышению квалификации специалистов по борьбе с преступлениями в сфере информационных технологий.

Нам представляется актуальным расширение такого рода сотрудничества в рамках различных программ построения и развития в стране информационного общества, противодействия терроризму и другим негативным проявлениям обще-

# Информационные технологии и безопасность в Национальном исследовательском ядерном университете «МИФИ»

ственной жизни. Университет имеет современную научную, учебно-методическую и учебно-лабораторную базу, обеспечивающую необходимый уровень образовательной и научной деятельности, богатый опыт и кадровый потенциал, которые являются основой эффективной работы университета. НИЯУ МИФИ готов расширить сферу взаимодействия в интересах МВД России. Определению возможных «точек» взаимодействия и посвящено данное сообщение.

## Немного истории

Практически с самого момента зарождения (в следующем году университет отмечает свое 70-летие) наряду с физическими подразделениями в МИФИ был создан факультет электронно-вычислительных устройств и средств автоматики. Основным предназначением подготовки специалистов этого факультета была разработка аппаратно-программных средств обеспечения устойчивой и безопасной работы ядерно-физических установок. В 60-х годах прошлого столетия в эпоху бурной компьютеризации факультет был разделен на два **относительно независимых подразделения**:

- автоматики и электроники — как база подготовки специалистов в области разработки аппаратных средств;
- кибернетики — как база подготовки в области информационных технологий.

В начале 90-х годов МИФИ одним из первых гражданских вузов страны отметил актуальность развития такого приоритетного в настоящее время научного направления, как информационная безопасность. В связи с этим в составе факультета кибернетики было выделено отдельное подразделение — факультет информационной безопасности, который за очень короткое время стал признанной школой в системе высшего образования.

Но время берет свое — статус национального исследовательского ядерного университета потребовал внесения новых структурных корректировок, отражающих современные потребности развития науки и техники. Так родилась парадигма подготовки специалистов не только по безопасным информационным технологиям, но и разработки соответствующих информационных технологий для уполномоченных организаций сферы обеспечения безопасности личности, общества и государства. В связи с этим в этом году два профильных факультета объединены в единую структуру кибернетики и информационной безопасности, что на наш взгляд будет способствовать решению крупных комплексных проектов в области информационных технологий и безопасности. На наш взгляд, для этого новый факультет имеет все необходимые предпосылки, материально-технический и кадровый потенциал.

Приведем некоторые примеры возможных сфер взаимодействия НИЯУ МИФИ с организациями МВД России в области информационных технологий и безопасности.

## Образовательная деятельность

В рамках этой сферы наиболее приемлемой «точкой» взаимодействия является целевая элитная подготовка молодых специалистов. НИЯУ МИФИ имеет лицензии на образовательную деятельность по следующим направлениям (специальностям), имеющим отношение к информационным технологиям, связи и защите информации:

- 230100 — информатика и вычислительная техника;
- 230700 — прикладная информатика;
- 231300 — прикладная математика;
- 230106 — применение и эксплуатация автоматизированных систем специального назначения;



- 090900 — информационная безопасность;
- 090303 — информационная безопасность автоматизированных систем;
- 090305 — информационно-аналитические системы безопасности;
- 090915 — безопасность информационных технологий в правоохранительной области.

В рамках этих направлений реализуются самые разнообразные учебные программы подготовки бакалавров, магистров и специалистов, что позволяет отслеживать изменения требований к квалификации выпускников со стороны организаций, являющихся заказчиками и работодателями молодых специалистов.

#### Примеры таких учебных программ:

1. Подготовка бакалавров по программе (профиль) «Комплексная защита объектов информатизации» (направление подготовки 090900). Объектами профессиональной деятельности выпускника по данной программе являются компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере, технологии обеспечения информационной безопасности, используемые на таких объектах, а также технологии аттестации уровня их защищенности.
2. Подготовка специалистов по специальности 090303 (специализация «Безопасность открытых информационных систем»). Объектами профессиональной деятельности выпускника по данной специальности являются так называемые открытые информационные системы (ОИС), функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите, информационные технологии, формирующие информационную инфраструктуру ОИС (к таким технологиям относятся, например, интернет-технологии), а также технологии обеспечения информационной безопасности ОИС.

3. Подготовка специалистов по специальности 090305 (специализация «Информационная безопасность финансовых и экономических структур»). Объектами профессиональной деятельности выпускника по данной специальности являются специальные автоматизированные информационно-аналитические системы, обеспечивающие поддержку принятия решений в процессе организационного управления, в том числе специальные автоматизированные информационно-аналитические системы в сфере противодействия легализации («отмыванию») доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ), модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе: технологии, методы и средства ПОД/ФТ, системы государственного финансового мониторинга, а также системы финансового мониторинга в кредитных и некредитных организациях и системы международного финансового мониторинга.

Практически по всем указанным выше направлениям образовательной деятельности имеется богатый опыт обучения в рамках дополнительного образования, в том числе в аспирантуре и докторантуре по соответствующим научным специальностям, в частности по специальности 05.13.19 — методы и системы защиты информации, информационная безопасность.

О возможностях НИЯУ МИФИ в этом направлении говорит статистика: за 15 лет с момента создания факультета информационной безопасности на его базе прошли обучение более 10 000 специалистов Банка России и других крупнейших банков страны — Сбербанк, ВТБ, Внешэкономбанк.

#### Научная работа

Образовательная деятельность в МИФИ всегда поддерживалась серьезными научными исследованиями по самым приоритетным и прорывным технологическим направлениям. Это же касается и информационных технологий и обеспечения безопасности страны.

Как правило, они проводятся по специальной тематике, но и сфера открытых систем не остается без внимания. В качестве примера приведем разработку средств противодействия атакам на мобильные телефоны с помощью SMS-шлюзов.

С ростом функциональных возможностей мобильных телефонов увеличивается диапазон угроз, которым подвержены их владельцы. Эти угрозы направлены на перехват конфиденциальной информации, получение финансовой выгоды и вывод устройств из строя. SMS-спам мобильных телефонов — достаточно редкое явление в настоящее время, но весьма эффективное, если целью злоумышленника является отключение функции приема текстовых сообщений мобильного устройства пользователя.

Данной проблеме не уделяется должного внимания со стороны сотовых операторов. Дело в том, что обнаружить подобную атаку и закрыть подозрительный SMS-шлюз достаточно легко, и считается, что защита в данном случае осуществляется со стороны SMS-шлюза, так как для него подобные атаки просто невыгодны. Тем не менее существует целый ряд сервисов, расположенных преимущественно в развивающихся странах, в странах Ближнего Востока, позволяющих регистрацию пользователей без предоставления паспортных данных и без какого-либо контроля их деятельности. Поэтому даже в случае обнаружения факта проведения атаки невозможно привлечение злоумышленника к ответственности.

Нашим молодым ученым удалось найти достаточно эффективное решение данной проблемы, чему будет посвящена отдельная статья.

В заключение хочется выразить надежду на расширение и создание устойчивого взаимодействия одного из ведущих российских университетов с организациями МВД России, что несомненно будет способствовать развитию кадрового потенциала государственной системы обеспечения безопасности страны.