ОСНОВНЫЕ ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

А.А. Несмеянов,
старший преподаватель кафедры
автотехнической
экспертизы и автоподготовки,
ФГКОУ ВПО ВИ МВД России,
кандидат физико-математических наук,
доцент

В статье рассматриваются проблемные вопросы борьбы с преступлениями в области высоких технологий, дается анализ существующего положения дел и поднимается тема подготовки квалифицированных специалистов в области компьютерной безопасности в образовательных учреждениях МВД России.

The article deals with the problematic issues of combating crime in the area of high technology, analyzes the current state of affairs in the world and raises a question of training qualified specialists in the field of computer security in educational institutions of the Ministry of Internal Affairs of Russia[*].

Сегодня в результате быстрого развития компьютерных технологий и активного расширения их применения в различных сферах жизни человечество вошло в новую эру информатизации, когда компьютер является необходимым инструментом в самых различных областях деятельности человека. Мы можем, например, элементарно общаться или совершать многомиллионные денежные операции с людьми с другой стороны планеты и делать это быстро и недорого. Постоянное увеличение количества персональных компьютеров, свободный доступ к Интернету и динамично развивающийся рынок новых коммуникационных устройств изменили как способы проведения досуга, так и методы ведения бизнеса.

Однако любая медаль имеет обратную сторону. Доступность глобальных цифровых технологий открыла новые возможности и преступному сообществу. Ежедневно обладающие компьютерными знаниями и навыками преступники незаконно получают огромные денежные средства. Хуже того, глобальные компьютерные сети также используются с целью разжигания национальной розни, способствуют усилению экстремизма и сепаратизма, достаточно часто применяются для координации и осуществления террористических актов. К глубокому сожалению, во многих случаях правоохранительные органы отстают от преступников, испытывая недостаток как технических средств, так и, что особенно важно, квалифицированного персонала для отражения новой и быстрорастущей угрозы киберпреступности (понятие, объединившее преступления, связанные

[*] Nesmeyanov A. Main problems of combating crimes in high-tech

с использованием компьютерной техники, информационных технологий и глобальных сетей).

Рассмотрим краткую классификацию киберпреступлений в зависимости от объекта, предмета посягательства и от способов совершения. Наиболее распространенная классификация киберпреступлений основывается на Конвенции Совета Европы о киберпреступности [1] и изначально подразделяла их на четыре группы, затем был принят дополнительный протокол, и теперь групп – пять:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, такие как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему.
2. Преступления, связанные с использованием компьютера как средства совершения преступлений. В эту группу входят компьютерное мошенничество и компьютерный подлог.
3. Преступления, связанные с содержанием данных, размещенных в компьютерных сетях (контентом).
4. Преступления, связанные с нарушением авторского права и смежных прав.
5. Преступления – акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

До недавнего времени в мире не придавали большого значения исследованиям феномена киберпреступности и последствий её расширения. Во многих случаях работники правоохранительных органов ощущали недостаток инструментария, необходимого для того чтобы заняться этой проблемой. Старые законы недостаточно соответствовали совершаемым преступлениям, новые не могли наверстать упущенное и догнать действительность, имелось мало судебных прецедентов, которыми можно было бы руководствоваться. И, наконец, одной из важнейших проблем являлось отсутствие эффективного взаимодействия между двумя наиболее важными участниками процесса борьбы с киберпреступностью – сотрудниками правоохранительных органов и IT-профессионалами. Однако в последние годы ситуация стала меняться в лучшую сторону. Например, в 2013 г. в Гааге открылся Европейский центр по борьбе с киберпреступностью [2]. На сегодняшний день существуют ещё две крупные международные организации, активно работающие в этом направлении – подразделение по борьбе с терроризмом (Action Against Terrorism Unit) ОБСЕ, а также Интерпол, который заканчивает работу по созданию отделения по борьбе с киберпреступностью в Сингапуре, штат которого будет насчитывать более 200 сотрудников.

Во многих странах сейчас уже созданы особые группы реагирования на компьютерные инциденты (CERT, Computer Emergency Response Teams) и приняты специальные законы по противодействию киберпреступности. Однако, очевидно, что в наши дни задачи по борьбе с киберпреступностью не могут эффективно решаться какой-либо отдельной организацией. Преступления такого рода имеют практически неограниченную географию, а их жертвами могут стать пользователи в любой части света. Органы же

правопорядка имеют достаточно ограниченную юрисдикцию и не могут самостоятельно проводить расследования на территории других государств. Поэтому организация эффективного сотрудничества на международном уровне совершенно необходима.

В качестве примера здесь можно привести сотрудничество получившей широкую известность в России «Лаборатории Касперского» с Интерполом и международной организацией многостороннего сотрудничества против киберугроз (Multilateral Partnership Against Cyber Threats), которая является подразделением Международного союза электросвязи ООН [3]. Первая предоставляет наиболее актуальные технические данные о широко распространенном или опасном вредоносном ПО, которые при содействии Интерпола и IMPACT могут быть использованы в ходе текущих расследований или для возбуждения новых дел.

Также в рамках действующих соглашений «Лаборатория Касперского» предоставляет свои сервисы и экспертизу по обнаружению угроз, а её технологическая база будет использоваться в лаборатории цифровой криминалистики уже упомянутого отделения по борьбе с киберпреступностью в Сингапуре. Кроме того, постоянно проводятся тренинги для офицеров Интерпола с целью передачи опыта в вопросах анализа вредоносных программ, обнаружения цифровых следов и улик, а также исследования финансовых угроз.

Генеральным секретарем Интерпола Р. Ноублом по поводу данного сотрудничества было сказано следующее [3]: «…Сложные и постоянно эволюционирующие киберугрозы требуют высокого уровня технической экспертизы, и поэтому в вопросе противодействия киберпреступности правоохранительным органам крайне важно заручиться поддержкой специалистов из разных секторов. Соглашение между Интерполом и «Лабораторией Касперского» – серьезный шаг в сторону глобального объединения усилий в борьбе с киберпреступностью и достижения уверенности в том, что мы предлагаем вверенным нам государствам самые современные средства обеспечения безопасности…».

Также, например, сравнительно недавно инновационным центром «Сколково» был выделен грант компании Group-IB для разработки глобальной системы противодействия киберпреступности CyberCop, представляющей собой комплекс инструментов, направленный на выявление и нейтрализацию неправомерных действий в виртуальном пространстве и содержащей в своей основе технологию глобального мониторинга, сбора и анализа данных о способах подготовки и совершения киберпреступлений, выявления закономерностей и выработки алгоритмов превентивных мер, а также механизмов фиксации фактов и следов преступлений в Сети.

Еще одним примером существующего взаимодействия правоохранительных органов и IT-компаний может служить открытый корпорацией Microsoft Центр по борьбе с мировой киберпреступностью. Его работа направлена на противодействие онлайн-преступлениям, распространению вредоносных программ, нарушению прав интеллектуальной собственности и т.п.

Отделения Центра используют все технологии Microsoft, позволяющие бороться с глобальными киберугрозами в режиме реального времени. Например, технология SitePrint поможет отследить местонахождение киберперступников, программа PhotoDNA позволит оградить ребенка от запрещенных сайтов в Сети.

В Центре имеется отдельный департамент для работы со сторонними партнерами, который дает возможность сотрудникам правоохранительных органов и экспертам по кибербезопасности со всего мира взаимодействовать со специалистами Microsoft в режиме реального времени.

«В борьбе с киберпреступностью на уровне государства опыт частных компаний, таких как Microsoft, имеет большое значение – он позволяет эффективней защищать граждан от преступлений в интернете, – сказал Н. Накатани, исполнительный директор Interpol Global Complex for Innovation [4]. – Чтобы опережать преступников, сообщество специалистов по компьютерной безопасности должно действовать скоординированно. Благодаря Центру Microsoft по борьбе с киберпреступностью выполнение этой задачи будет более эффективным».

Сегодня не существует ни релевантной статистики, позволяющей проанализировать данные, отражающие реальную картину состояния киберпреступности, ни надежных методов сбора таких данных, поэтому нельзя сказать, до какой степени достоверна статистика об экономических потерях в результате совершения преступлений такого рода. Существует мнение, что доходы от киберпреступлений в последние годы превышает даже доходы от незаконного оборота наркотических веществ и оружия. Анализ результатов исследований, приведенный в 2013 г. американским Центром стратегических и международных исследований и компанией McAfee [5], показывает, что ежегодные потери мировой экономики от киберпреступлений и их последствий достигли уже рекордной цифры в 500 млрд долларов, что сопоставимо с бюджетом средней европейской страны. Доля России в этой печальной статистике более миллиарда долларов. Тут необходимо отметить, что структура киберпреступности в разных странах заметно различается в зависимости от характера и степени развития информационных технологий, распространения сети Интернет, использования электронных сервисов, электронной коммерции и т.п. Например, в США 44 % такого рода преступлений составляют кражи денег с электронных счетов, 16 % – повреждения программного обеспечения, столько же – похищение секретной информации, 12 % – фальсификация информации, 10 % – заказ услуг за чужой счет. Структура российской компьютерной преступности рассматривается, например, в [6, с. 548-589].

Приведенные факты еще раз доказывают необходимость обеспечения правоохранительных органов грамотными специалистами в области АТ-технологий. Сегодня эту нишу занимают в основном люди, пришедшие после окончания гражданских вузов, поэтому одним из важных направлений развития образования в МВД является обучение специалистов именно по данному направлению.

Как уже отмечалось ранее [7], в ряде образовательных организаций МВД такие специальности уже открыты. Так в Московском университете МВД России существует факультет подготовки специалистов в области информационной безопасности. Постоянно проводятся научно-практические конференции по технологиям информационной безопасности в деятельности органов внутренних дел. На них представляются результаты научных разработок от развития представлений о технических каналах утечки информации, электромагнитного экранирования служебных кабинетов, использования генераторов акустического шума, применения тепловизоров до космических навигационных технологий, технологий радиочастотной идентификации, использования компьютерной стеганографии, а также технологий безопасного электронного документооборота, повышения качества подготовки специалистов, криминогенного потенциала ресурсов Интернета и информационного противоборства [8]. В Санкт-Петер-бургском и Краснодарском университетах МВД России существуют специальности «Организация и технология защиты информации», «Информационные системы и технологии», специалистов-электрон-щиков готовят в рамках специальностей «Применение и эксплуатация автоматизированных систем специального назначения», «Инфокоммуникационные технологии и системы специальной связи» в Воронежском институте МВД России.

На территории же Сибири и Дальнего Востока подготовка специалистов необходимого профиля практически не ведется, хотя потребность в них сейчас велика. В образовательных организациях МВД наших регионов изучаются только отдельные предметы, такие как «Информационная безопасность и применение информационных технологий в борьбе с преступностью», «Информационная безопасность и применение информационных технологий в юриспруденции», «Защита информации», «Расследование преступлений в сфере компьютерной информации и высоких технологий». Таким образом, открытие новых специальностей по данному направлению, или хотя бы введение дополнительных профильных специальных дисциплин является достаточно актуальным на сегодняшний день.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Волеводз А.Г. Конвенция о Киберпреступности: Новации Правового Регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17–25.

2. European Cybercrime Centre URL: https://www.europol.europa.eu/ec3 (дата обращения: 30.11.14).

3. Официальный сайт «Лаборатории Касперского» URL: www.kaspersky.ru (дата обращения: 29.11.14).

4. Официальный сайт американского Центра стратегических и международных исследований URL: http://usinfo.state.gov (дата обращения: 29.11.14).

5. Официальный сайт независимого информационного интернет-агентства URL: http://www.innovanews.ru (дата обращения: 29.11.14).

6. Развитие российского общества: социально-экономические и правовые исследования: монография / под ред. М.А. Винокурова, А. П. Киреенко, С. В. Чупрова. – М.: Издательский Дом «Наука», 2014. – 622 с.

7. Несмеянов А.А., Подопригора А.Г. Подготовка специалистов в области информационной безопасности как важнейшее направление в системе профессионального обучения сотрудников полиции // Вестник Восточно-Сибирского института МВД России. – 2011. – №5 (56). – С. 12-17.

8. Официальный сайт Московского университета МВД России URL: http://mosumvd.com (дата обращения: 29.11.14).