подхода к их принятию и реализации. Для предупреждения и пресечения преступлений в сфере охраны культурного наследия необходимо продолжить реформирование системы охраны объектов культурного наследия, повышать ее эффективность, готовить соответствующих специалистов, а также обеспечить возможность их взаимодействия с ОВД. Дальнейшее изучение проблемы охраны культурного наследия актуально для последующей практической работы государства и гражданского общества в данной области.

[1] Лихачев Д.С. Письма о добром и прекрасном (письмо № 40-41. О памяти). М., 1985. С. 45.

[2] Сведения из Единого государственного реестра объектов культурного наследия (памятников истории и культуры) народов Российской Федерации. URL: http://opendata.mkrf.ru/ opendata /7705851331-egrkn (дата обращения: 27.07.2018).

[3] Милежик А.В. Охрана археологических памятников на территории Дальнего Востока России : справочное пособие. ДВЮИ МВД России. Хабаровск, 2015. 100 с.

[4] Судебный департамент при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 27.09.2018).

[5] Усов А.В. Особенности привлечения к юридической ответственности за причинение вреда памятникам истории и культуры Российской Федерации // Вестник ДВЮИ МВД России. 2014. № 1 (26). С. 63-70; Кулажников В.В., Милежик А.В., Усов А.В. Современное состояние уголовно-правовой охраны культурного наследия на территории Приморского края // Реформа уголовного законодательства в Российской Федерации (к 20-летию Уголовного кодекса Российской Федерации) : материалы всероссийской научно-практической конференции (Владивосток, Дальневосточный юридический институт МВД России). Хабаровск : РИО ДВЮИ МВД России, 2017. С. 114-121.

Салахова Ж.В.,

кандидат юридических наук, доцент
Уфимский юридический институт МВД России

Преступления в сфере компьютерной информации

Компьютерная преступность – совокупность преступлений, в которых предметом преступных посягательств является компьютерная информация. С позиций уголовного законодательства это преступления в сфере компьютерной информации. В настоящее время законодатель выделяет в УК РФ четыре общественно опасных деяния в сфере компьютерной информации: ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, ст. 273 УК РФ – за создание, распространение и использование вредоносных программ для ЭВМ, ст. 274 УК РФ – за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, ст. 274.1. – за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (введена Федеральным законом от 26 июля 2017 г. № 194-ФЗ, вступил в силу с 1 января 2018 г.).

В 2017 году Российская Федерация столкнулась практически со всеми актуальными видами кибератак. Кибератака – это попытка внести изменения в работу компьютерных систем или сетей, вывести их из строя, разрушить, а то и уничтожить информацию или программы, которые в них хранятся или какие они передают. С каждым годом они становятся все сложнее и изощреннее. За 2017 год 85% пользователей Интернета в России подвергались вирусным или иным атакам. В то же время **33%** владельцев мобильных устройств считают, что удобство постоянного нахождения в Интернете перевешивает любые угрозы безопасности, а **57%** опрошенных даже не знают, что решения по обеспечению безопасности мобильных устройств существуют.

С 2013 по 2017 год число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, увеличилось до

66 тыс. ежегодно. Это порождает необходимость повышения эффективности работы правоохранительных органов в сфере противодействия киберпреступности.

В 2017 году более 2/3 преступлений экстремистской направленности и каждое девятое преступление террористического характера были совершены с использованием Интернета.

Компьютерная преступность системно взаимосвязана с иными видами преступности. Компьютерные преступления могут совершаться совместно практически со всеми преступлениями и против всех объектов уголовно-правовой защиты. Так, исполнение многих общественно опасных деяний, например мошенничества, вымогательства, причинения значительного имущественного ущерба и даже убийства, достигается либо облегчается посредством преступных посягательств на компьютерную информацию.

Можно выделить следующие виды общественно опасных деяний, при совершении которых наиболее часто компьютерные преступления служат средством достижения общественно опасных последствий.

Общественно опасные деяния против прав и свобод человека и гражданина, прав и законных интересов юридических лиц. Наиболее распространенным преступлением такого рода является компьютерное пиратство. Оно заключается в незаконном копировании и распространении программ для ЭВМ и баз данных, причиняя существенный вред правоотношениям, возникающим в связи с созданием, правовой охраной и использованием программ для ЭВМ и баз данных. Следует отметить, что подобного рода преступления наносят значительный ущерб экономике.

Крайне опасным явлением в России стало незаконное копирование и массовое распространение автоматизированных информационных баз данных, содержащих информацию о номерах телефонов, адресах граждан и юридических лиц, автотранспортных средств, находящихся в собственности, недвижимости и т.д. Общественная опасность таких действий заключается в нарушении конституционных прав граждан, коммерческих интересов организаций. Похищенные базы данных часто используют для совершения других преступлений, например в сфере экономики.

Серьезную общественную опасность представляют действия спамеров – лиц, осуществляющих массовую рассылку различного рода информации в виде электронных сообщений людям без их согласия.

В настоящее время около 80% писем в Интернете составляет спам. По некоторым данным на одного интернет-пользователя сегодня приходится по 70 спам-сообщений в сутки.[1]

Общественно опасные деяния с использованием компьютерной информации в сфере экономики. В настоящее время во всех сферы жизни человека внедрены автоматические системы, которые контролируются и программируются компьютером. Самый большой ущерб наносят различные формы хищений путем незаконного доступа в автоматизированные системы различных учреждений.

В 2000-х гг. масштабы совершения компьютерных преступлений с участием технического персонала организаций настолько возросли, что сотрудники служб безопасности дали название этому персоналу – «инсайдеры». Следует отметить, что они часто совершают преступления не только из корыстных побуждений, но и, например, из мести.

Чаще всего инсайдеры-вредители совершают действия, направленные на сбои в системе коммуникаций, остановку продаж, уничтожая программное обеспечение, отвечающее за электронную реализацию товара. Внося изменения в существующие базы данных (меняя пароли), они создают серьезные проблемы владельцам и пользователям.

Данные действия часто совершаются и в целях вредительства, и в целях вымогательства, становясь все более изощренными. В компьютер жертвы по Сети или с помощью инсайдеров внедрялись вредоносные программы, которые активировались в соответствующий момент и блокировали работу системы. Преступников можно было вычислить только в

момент, когда они звонили с требованием о переводе денег. Еще позже появились вредоносные программы, которые блокировали работу ЭВМ и самостоятельно информировали жертву о необходимости срочно перевести деньги на определенный счет. В таких случаях задержать преступников можно только при получении денег, что весьма затруднительно, если учесть возможности систем электронных платежей перевести деньги быстро и в любую точку планеты.

В конце XX – начале XXI вв. появилось большое количество новых общественно опасных явлений, в частности фишинг – мошенничество. Фишинг (англ. *fishing* – рыбная ловля, выуживание) – вид интернет-мошенничества, цель которого – получить идентификационные данные пользователей.[2]

В это же время появились факты и так называемого фрода, т.е. действий по незаконному использованию услуг оператора. Это неправомерное использование чужих идентификационных данных для доступа в Интернет, другие сети, базы данных. К этим действиям относятся и различные незаконные способы доступа к персональным данным пользователей (абонентов) сотовыми телефонами и их использования для получения платных услуг международной связи. Среди мошенников это называется «учредить переговорный пункт».

Появились случаи использования преступниками создаваемой ими масштабной сети так называемых зомби-компьютеров, т.е. ЭВМ третьих лиц, которые и не подозревают, что с их компьютера могут осуществляться различного рода преступления.

Обычно случаи неправомерного доступа к компьютерной информации или создания вредоносных компьютерных программ являются частью более глобальных мошеннических преступных схем, реализуемых международными преступными группами.

Таким образом, преступность в сфере компьютерной информации, будучи относительно недавно сформировавшимся видом, находится в стадии динамического и ускоренного развития.

Регулярно осуществляются атаки на российские банки, в ходе которых их сетевая инфраструктура бывает полностью парализована. Слаженные действия сотрудников Управления «К» МВД России во взаимодействии с Центробанком России позволяют предотвратить значительный материальный ущерб кредитно-финансовым учреждениям.

Преступные группы, совершающие кибератаки, отличаются высоким уровнем подготовки и технического оснащения, они хорошо законспирированы и, как правило, действуют на территории сразу нескольких регионов страны. Целью преступников все чаще становятся не клиенты банков, а непосредственно финансовые учреждения и объекты информационной инфраструктуры государства.

Однако не все преступления имеют корыстные мотивы. Отдельным направлением работы правоохранительных органов является защита детей в Сети и противодействие изготовлению и распространению детской порнографии.

К преступлениям против общественной безопасности относят также неправомерный доступ к компьютерному обеспечению деятельности, создающей повышенную опасность для окружающих. Компьютерные технологии широко используются в вооруженных силах, космической отрасли, атомной энергетике, наземном, морском и воздушном транспорте и т.д.

Такие действия представляют угрозу обороноспособности любой страны, способны привести к возникновению опасных аварийных ситуаций, экологическим катастрофам, многочисленным жертвам. Кроме того, тяжкие последствия и существенный вред могут быть получены вследствие нарушения правил эксплуатации ЭВМ или их сетей, которые применяются в деятельности, имеющей повышенную опасность.

[1] URL: http://www.wikipedia.org (дата обращения 10.09.2018).

[2] URL: .http://dic.academic.ru/dic.nsf/ruwiki/977065. (дата обращения 12.09.2018).