Секция «Информационное общество, цифровая экономика и информационная безопасность»

АНАЛИЗ СОСТОЯНИЯ КИБЕРПРЕСТУПНОСТИ И МЕТОДОВ БОРЬБЫ С НЕЮ В СТРАНЕ

Научный руководитель – Серезевский Алексей Вадимович

Ремидовская Ирина Александровна

Студент (специалист)

Московский университет Министерства внутренних дел Российской Федерации, Факультет подготовки специалистов в области информационной безопасности, Москва, Россия

E-mail: remidovskaya.irina@yandex.ru

Впервые использование компьютера как инструмента для совершения кражи было зафиксировано в 1966 году в Миннесоте, США. Тогда это был первый случай, когда компьютер был официально признан техникой для совершения преступления, это и ознаменовало наступление эры высокотехнологичной преступности. С того момента преступления с использованием информационно-телекоммуникационных технологий получили широкое распространение практически во всех сферах деятельности человека и общества в целом.

Современное общество повсеместно использует различные достижения науки. В настоящее время человек вряд ли сможет прожить без компьютеров, телекоммуникационных систем и глобальной сети Интернет, так как эти технические новинки стали неотъемлемой частью жизни. Именно это и сформировало новый вид преступности - киберпреступность. Порой положительные качества Интернета используют не для благих целей. Для преступников, которые работают в сети, интернет может играть несколько ролей. Его возможности позволяют злоумышленнику совершить преступления разной направленности. С одной стороны, Интернет можно рассматривать как вспомогательное средство. В другом же случае, он может играть роль места совершения преступлений, таких как: кража, вымогательство, мошенничество и т.д.

По мнению экспертов Организации Объединенных Наций, термин «киберпреступность» подразумевает любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети. Следовательно, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

С каждым годом развитие информационно-коммуникационных технологий влечет за собой рост количества преступлений в данной сфере. Можно отметить, что киберпреступность, на данный момент, занимает лидирующие позиции в отношении прироста. Причины, объясняющие это явление, могут быть неоднозначны. Я считаю, что такие факторы как разработка новейших материально-технических и программно-аппаратных средств в области IT-индустрии, постоянное увеличение пользователей глобальной сети Интернет, совершенствование знаний и умений киберпреступников, связанных с использованием различных технических и программно-аппаратных средств для совершения преступления, могут являться причиной роста популярности данного вида преступлений. Преступники эффективно совершенствуют имеющиеся достижения науки, тем самым повышают уровень эффективности хакерских атак.

При анализе докладов Международного союза электросвязи (МСЭ) можно отметить, что в 2000 году число пользователей глобальной сети Интернет составляло примерно 400

млн. человек, а в настоящее время их число резко возросло и достигло отметки в 4,39 млрд. человек, что составляет 53% населения Земли.

В связи с развитием различных технологий, киберпреступность стала одной из главных проблем, при этом ущерб от данного вида преступлений может быть нанесен не только отдельным гражданам, деятельность которых связана с непосредственным взаимодействием с информационно-телекоммуникационными системами и технологиями, но и всему обществу и государству. Инновационное вредоносное программное обеспечение предоставляет злоумышленнику возможность реализации их функций в качестве орудий или средств совершения преступлений, закрепленных в нормативно-правовых актах законодательной ветви власти Российской Федерации. Возможность интегрирования таких программ позволяет трансформировать их функции, что приводит к расширению возможностей программного обеспечения. Именно поэтому деятельность киберпреступников можно признать одним из опасных видов преступности.

В связи с резким увеличением уровня киберпреступности, по всей России появляется потребность в создании и функционировании различных специализированных подразделений и групп, задачами которых является расследование преступлений в сфере «высоких технологий», а следствие и их раскрытие. Деятельность преступника при совершении такого вида преступлений обычно связана с использованием различных видов вредоносных материально-технических и программно-аппаратных средств. Работа специальных подразделений связана с фиксацией, юридическим оформлением выявленного преступления, а также ведением статистики по различным квалификациям преступного поведения. Несмотря на активную деятельность сотрудников, эффект минимален, а сдержать каким либо образом рост киберпреступности пока не представляется возможным. Причиной этому можно считать то, что работа этих подразделений ведется в основном с последствиями преступлений, а не с причинами возникновения. В итоге мы также наблюдаем рост киберпреступности и постоянное совершенствование и интегрирование вредоносного программного обеспечения и материально-технических средств, что является главным угрожающим фактором для борьбы с данным видом преступлений.

Согласно статистике Главного информационно-аналитического центра МВД РФ, за период январь-декабрь 2019 года было зарегистрировано 2944409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что по сравнению с прошлым годом увеличилось на 68,5%. Тяжких и особо тяжких насчитывается 142728(прирост 149,0%).

При рассмотрении по квалификации можно заметить, что лидирующую позицию занимает мошенничество (ст. 159 УК РФ). Также резко возросло количество преступлений: кража (ст. 158 УК РФ) и мошенничество с использованием платежных карт (ст. 159.3 УК РФ).

Немалую часть занимают преступления, квалифицируемые по статье 228.1 УК РФ «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества».

Уменьшилось количество преступлений по квалификации: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ); незаконные организация и проведение азартных игр (ст. 171.2 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Заключение

С каждым годом применение информационно-телекоммуникационных технологий становится наиболее актуальным орудием совершения преступлений различной направленно-

сти. Деятельность киберпреступников направлена на причинение ущерба различным субъектам правоотношений: отдельным гражданам, организациям, предприятиям и т.д. Причем риск преступника сводится к минимуму. Злоумышленники просчитывают свои действия на опережение, именно это значительно увеличивает нагрузку на работу систем безопасности. Для решения проблемы киберпреступности стратегия компаний должна заключаться не в том, чтобы приспосабливать систему безопасности под существующие тенденции совершения преступлений, а в активной разработке средств и методов защиты предприятия, которая заключается в действии на опережение.