СРАВНИТЕЛЬНЫЙ ОБЗОР МЕЖДУНАРОДНОГО ОПЫТА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В КОМПЬЮТЕРНОЙ СФЕРЕ

Жилинкова Людмила Анатольевна

доцент кафедры философии,

социально-правовых и естественнонаучных дисциплин,

Курская академия государственной и муниципальной службы, г.Курск

Иванова Анна Николаевна

старший преподаватель кафедры философии,

социально-правовых и естественнонаучных дисциплин,

Курская академия государственной и муниципальной службы, г.Курск

В рамках современных реалий сформировался новый вид общественных отношений – информационные, а главным символом XXI века по праву можно считать информацию. Можно констатировать, что если раньше темпы развития человечества определялись доступной ему энергией, то теперь – доступной ему информацией.

Сегодня мы наблюдаем стремительное развитие и внедрение компьютерных и информационных технологий практически во всех сферах жизнедеятельности человека, предприятий и государства. Вопросы защиты в сфере компьютерной информации, в том числе, персональных данных становятся все более актуальными и требующими решения в ближайшей перспективе.

Компьютерные преступления носят большой материальный и портит имидж, а так же несут реальную угрозу экономики предприятия, государства. И тем не менее практически все виды таких преступлений реально предотвратить. Накопленный мировой опыт говорит о том, что для решения поставленного вопроса необходимо принимать различные профилактические меры, направленные на выявление и устранение причин возникновения преступления, и условий, способствующих их совершению.

Англо-саксонская правовая система.

США.

1977 год – США разработали законопроект о защите федеральных компьютерных систем.

1984 год – США принят закон о мошенничестве и злоупотреблении с использованием компьютеров. В последующем неоднократно дополнялся и на сегодняшний день включен в виде §1030 47 -ой главы в Титул 18 Свода законов США.

1986 год - Закон «О мошенничестве и злоупотреблениях, связанных с компьютерами».

Великобритания.

1984 год – Закон о защите данных

1990 год - Закон о неправомерном использовании компьютерных технологий (Computer Misuse Act), регулирующий отношения в информационной сфере.

1997 год - Закон о телекоммуникациях.

1998 год - Закон о защите персональных данных (Data Protection Act)

2000 год - Закон об электронном сообщении, Закон о телевизионных лицензиях (раскрытие информации)

2001 год - Закон о борьбе с обманом в области социального обеспечения

2003 год - Положение о частной информации и электронной связи 2003 г. (The Privacy and Electronic Communications (EC Directive) Regulations 2003)

Австралия. Основной документ, позволяющий обеспечивать противодействие компьютерным преступлениям это Уголовный кодекс [2-3].

Канада.

В уголовном кодексе отдельные положения законодательства в сфере компьютерных преступлений сформулированы в виде соответствующих поправок и дополнений к действующей системе уголовного права. В УК Канады сформулирован перечень компьютерных преступлений, среди которых: противоправное несанкционированное получение, непосредственно или косвенно, любых компьютерных данных и услуг; несанкционированный

перехват, прерывание, отслеживание и запись компьютерных данных; умышленное распространение бессмысленных, бесполезных или безрезультативных компьютерных данных и программ и другие.

Романо-германская правовая система.

Германия.

1986 год – внесение изменений в УК ФРГ и установление ответственности за компьютерные преступления.

Франция.

1994 год – вступивший в силу уголовный кодекс предусматривает ответственность за ряд компьютерных преступлений: перехват, хищение, использование сообщений, незаконный доступ к данным и другие.

Нидерланды.

1993 год – Закон о компьютерных преступлениях, дополняющий Уголовный кодекс новыми составами: несанкционированный доступ, копирование, распространение вирусов и другие.

Испания.

В УК Испании (действует с 1996 года) отсутствуют специальные нормы ответственности за преступления в сфере компьютерной информации. Вместо этого ответственность предусматривается лишь за преступления, совершаемые с использованием информационных технологий. Например: распространение тайных сведений, коммерческой тайны, посягательство на интеллектуальную собственность, подделка документов и другие.

Законодатель указанных стран обращает особое внимание противодействию указанным противоправным деяниям. Свидетельством этому является принятые нормативно-правовые акты.

В странах англо-саксонской правовой системы параллельно нормативно-правовым актам реализуется организационно-правовые меры, позволяющие не только упорядочить, но и повысить эффективность и результативность деятельности правоохранительных органов.

А вот характерной особенностью романо-германской правовой системы является установление ответственности в виде штрафа или лишения свободы.

Что касается портрета киберпреступника. Автор статьи [1] приводит следующие примеры существующих классификаций типов преступников. Четыре основных типа по В.В. Крылову:

1) нарушители правил пользования компьютерной техникой;

2) «белые воротнички» – респектабельные преступники;

3) компьютерные шпионы;

4) хакеры, или «одержимые программисты».

Классификация по Д. Паркеру:

1) pranksters – совершают преступления ради развлечения, без корыстных мотивов;

2) hucksters – лица с корыстными намерениями;

3) malicious hackers – злоумышленники;

4) personal problem solvers – лица, которые решают личные проблемы;

5) career criminals – профессиональные преступники;

6) extreme advocates – экстремалы, любители рисковать;

7) irrational people – «иррациональные люди».

Само собой центральным становится задача по обнаружению преступников и предотвращению их противозаконной деятельности. Поставленная задача сложна и многогранна в своем исполнении. Преступники становятся все более изобретательными, технологии стремительно развиваются и дает им в распоряжение еще больше инструментов. А новые защитные системы становятся новым вызовом для хакеров.

Как отмечает министр внутренних дел Великобритании Джек Стро: "Мы отстаем от преступников на один шаг, а должны быть на шаг впереди".

Важным фактором в деятельности, связанной с анализом и расследованием компьютерных преступлений выступает расширение и упрочнение сотрудничества с компетентными финансовыми структурами и подразделениями служб безопасности организаций.

Кроме того необходимо работать и по следующим направлениям:

1. Повышать правовое сознание, ответственность граждан.
2. Профессиональная переподготовка, постоянное повышение квалификации кадров в области обеспечения информационной безопасности.
3. Обеспечение взаимного сотрудничества правоохранительных органов разных государств. Обмен опытом и знаниями благоприятно скажется на борьбе с компьютерной преступностью.
4. Плотное сотрудничество с частными компаниями такими как: Google, Apple, Яндекс, Лаборатория Касперского и другие. У подобных компаний находятся целые арсеналы технологий по шифрованию и идентификации данных с помощью искусственного интеллекта.
5. Финансирование разработок технико-криминалистических средств, что значительно повысило бы эффективность расследования преступлений данной категории.

Список литературы

1. Ефремов К.А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. 2016. №6. С. 92-95.
2. Менжега М.М., Асаев А.Т. Проблемы расследования в сфере компьютерной информации // Научный электронный журнал Меридиан. 2020. № 3(37). С. 339-341.
3. Пелевина А.В. Ответственность за компьютерные преступления в романо-германской правовой системе // Пробелы в российском законодательстве. 2016. № 3. С. 76-79.
4. Пелевина А.В. Ответственность за компьютерные преступления в англо-саксонской правовой системе // Пробелы в российском законодательстве. 2016. № 1. С. 103-106.