Унанян Эдита Эдуардовна,
Студент бакалавр юридического факультета,
Российский государственный социальный университет,
г. Москва, Российская Федерация

Hunanyan Edita Eduardovna
The student of the bachelor of law faculty
Russian State Social University,
Moscow, Russian Federation

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЯ В РОССИИ

Responsibility for cybercrime in Russia

Аннотация: Мы очень часто слышим и читаем новости в которых рассказывается о новом взломе компьютерных систем, краже конфиденциальных данных, мошенничестве с финансами, утечки баз данных пользователей крупнейших интернет-магазинов или социальных сетей. Причем действия одних хакеров, например, группы Fancy Bears, которые взломали антидопинговое агенство WADA и опубликовали ряд документов, свидетельствующих о том, что американские атлеты на олимпиаде в Рио принимали запрещенные препараты, вызывают скорее симпатию, нежели чем желание их наказать. То же самое можно сказать и о взломах в результате которых материалы компрометирующие АНБ или ЦРУ были выложены на WikiLeaks. Однако не смотря на это компьютерный взлом и несанкционированный доступ к информации приравнивается к преступлениям, и как для любых других правонарушений, для них предусмотрены меры ответственности.

Ключевые слова: Ключевые компетенции, киберпреступления, защита информации.

Abstract: We very often hear and read news that tells about new hacking of computer systems, theft of confidential data, financial fraud, leaks of databases of users of the largest online stores or social networks. Moreover, the actions of some hackers, for example, the Fancy Bears group, who hacked the anti-doping agency WADA and published a number of documents indicating that American athletes took illegal drugs at the Rio Olympics, evoke sympathy rather than a desire to punish them. The same can be said about hacks, as a result of which materials incriminating the NSA or the CIA were posted on WikiLeaks. However, despite this, computer hacking and unauthorized access to information is equated with crimes, and as for any other offenses, measures of responsibility are provided for them.

Key words: Key competencies, cybercrimes, information protection.

Введение

В данной статье мы будем рассматривать научно технические преступления.

Мы очень часто слышим и читаем новости в которых рассказывается о новом взломе компьютерных систем, краже конфиденциальных данных, мошенничестве с финансами, утечки баз данных пользователей крупнейших интернет-магазинов или социальных сетей. Причем действия одних хакеров, например, группы Fancy Bears, которые взломали антидопинговое агенство WADA и опубликовали ряд документов, свидетельствующих о том, что американские атлеты на олимпиаде в Рио принимали запрещенные препараты, вызывают скорее симпатию, нежели чем желание их наказать. То же самое можно сказать и о взломах в результате которых материалы компрометирующие АНБ или ЦРУ были выложены на WikiLeaks. Однако не смотря на это компьютерный взлом и несанкционированный доступ к информации приравнивается к преступлениям, и как для любых других правонарушений, для них предусмотрены меры ответственности.

Ответственность за кибер преступления в России

В России разрешено свободное распространение информации при соблюдении всех требований, установленных законодательством Российской Федерации. Так базисным законом, регулирующим свободу доступа к информации, является ФЗ-149 "Об информации, информационных технологиях и защите информации". Данный законодательный акт призван регулировать отношения, возникающие между субъектами при

осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий, а так же обеспечении защиты информации.

Так же в законе сказано, что ограничение доступа к информации любого вида может устанавливаться федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Закон так же говорит: запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо его воли.

Такую информацию принято относить к Персональным данным, который регулирующий одноименный федеральный закон ФЗ-152 "О Персональных данных"

За более серьезные серьезные правонарушения предусмотена уголовная ответственность. Наиболее известный раздел в УК РФ это 28 глава, преступления в сфере компьютерной информации. Раздел включает в себя три статьи - 272, 273, 274.

Если же речь идет об использовании чужих логинов и паролей (фактически работа под чужой учетной записью), то в дела включаются еще и статьи ст.165 УК РФ "Причинение имущественного ущерба путем обмана или злоупотребления доверием", в некоторых случаях так же действия злоумышленника можно подписать под ст.183 УК РФ "Незаконное получение и разглашение сведений, составляющих коммерческую тайну", и банальная ст.159 УК РФ "Мошенничество".

Совсем недавно стало известно, что Сбербанк и Министерство внутренних дел (МВД) разработали совместный законопроект, который также был поддержан представителями Центробанка. Законопроект требует признать киберпреступления кражами, а не квалифицировать их как мошенничество, а также установить за их совершение более серьезное наказание.

Зарубежная практика в наказании кибер преступников

1. Законодательство США

Как известно первые ИТ компании зародились в США. Поэтому и первый законопроект, устанавливающий уголовную ответственность за

преступления в сфере информационных технологий, был разработан в США еще в далеком 1977 году. А уже позднее, на основе данного законопроекта в октябре 1984 года был принят закон о мошенничестве и злоупотреблении с использованием компьютеров (Computer Fraud and Abuse Act) .

Закон устанавливает ответственность за несколько основных составов преступлений: компьютерный шпионаж;

несанкционированный доступ к информации;

компьютерное мошенничество;

умышленное или по неосторожности повреждение защищенных компьютеров;

угрозы, вымогательство, шантаж, совершаемые с использованием компьютерных технологий и другие.

Ответственность за указанные кибер преступления предусматривают солидные денежные штрафы, а так же вполне реальное тюремное заключение. Наказание зависит от многих факторов, т.к. тяжесть совершенного преступления, размер экономического ущерба, причиненного деянием, криминального прошлого подсудимого и многих других.

Законодательство Великобритании

В туманном Альбионе с августа 1990 года действует Акт о компьютерных злоупотреблениях. Первый параграф этого документа касается "неуполномоченного доступа к компьютерным данным". Им установлено, что лицо совершает преступление, когда оно использует компьютер для выполнения любой функции с намерением обеспечить доступ к любой программе или данным, содержащимся в любом компьютере, если этот доступ заведомо неправомочен.

Так же стоит сказать о серьезности проблемы компьютерных преступлений это вступление в действие в соединенном королевстве Закона о терроризме 2000 года . В законе определение терроризма впервые расширяется до области киберпространства. К примеру, благодаря данному документу, английские правоохранительные органы вправе считать террористическими действия, которые "серьезно вмешиваются или серьезно нарушают работу какой-либо электронной системы".

Левин и крупнейший взлом Citibank

Действия происходили в 1994 году. Это ограбление стало первым в цепи противостояния российских хакеров и западного гиганта Citibank. Из материалов дела известно, что середине 1990-х годов петербуржец Владимир Левин проник во внутреннюю сеть американского банка, взломав аналоговое модемное подключение, и сумел перевести $10,7млн на счета в разные страны: США, Финляндию, Германию, Израиль и Нидерланды. Сообщники

выдали россиянина властям. После Левина арестовали в марте 1995 года в Лондоне, а через три года следствия приговорили к трем годам лишения свободы.

15-летний Джеймс нашел брешь в НАСА

На дворе уже 1999 год. И 15-летний хакер Джонатан Джеймс первым вскрыл систему Национального космического агентства США . Ему удалось получить доступ, взломав пароль сервера, принадлежащего другому правительственному учреждению, после чего Джеймс украл несколько важных файлов у НАСА, включая исходный код международной орбитальной станции. В тот момент агенство оценило ущерб в $1,7млн. Ввиду своего юного возраста Джеймс смог избежать тюрьмы.

Русский след и платежная система PayPal

Челябинские ребята, 26-летний Василий Горшков и его 20-летний друг Алексей Иванов были арестованы ФБР в ноябре 2000 года в Сиэтле. Их обвинили в незаконном проникновении в корпоративные компьютерные сети PayPal, Western Union, а также американского банка Nara Bank. С домашних компьютеров злоумышленники украли 16 тысяч номеров кредитных карт, чем причинили ущерб на $25млн. В итоге Иванов получил четыре года тюрьмы, а его подельник Горшков – три, но с обязательством выплатить $700 тысяч компенсации.

Снова русские хакеры против американской биржи

И вот уже 2013 год. В июле 2013 года власти США предъявили обвинения в мошенничестве и взломе компьютерных сетей пяти гражданам России и одному жителю Украины. Как утверждает следствие, речь идет об «одном из крупнейших киберпреступлений в истории». Обвиняемым удалось взломать системы безопасности электронной биржи NASDAQ , крупнейших торговых сетей и ведущих банков Европы и США. В результате были похищены данные 160 млн кредитных карт и сняты средства с 800 тысяч банковских счетов по всему миру. Перед судом в Ньюарке предстал только москвич Дмитрий Смилянец, он был арестован по запросу ФБР в Нидерландах. Остальным участникам гуроппы удалось скрыться и избежать наказания.

Таким образом мы видим, что в наше время хакеры имеют большие возможности для развития.данная тема очень актуальна, так как от их взломов никто не застрахован, как государственные деятели так и обычные люди.

Библиография:

1. Никодимов И.Ю АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА. Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2016. № 1 (763). С. 147-160.
2. Новиков М.Ю., Никодимов И.Ю. ЮРИСПРУДЕНЦИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В сборнике: УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ И НАКАЗАНИЕ.ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН. сборник статей по материалам научно-практической конференции. 2019. С. 160-166.
3. Сапожникова Е.С., Никодимов И.Ю. РОСТ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В сборнике: Правовое и криминалистическое обеспечение судебного исследования преступлений. Сборник статей по материалам Общероссийской конференции, посвященной памяти проф. В.В. Колкутина. Под редакцией В.Ю. Голубовского. 2019. С. 120-124.
4. Никодимов И.Ю. НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДМЕТА ИНФОРМАЦИОННОГО ПРАВА Правовое поле современной экономики. 2015. № 12. С. 135-140.
5. Гоголь А.А., Никодимов И.Ю. СТРАНИЦЫ ИСТОРИИ РАДИОСВЯЗИ (КОНЕЦ XIX – ПЕРВАЯ ЧЕТВЕРТЬ XX В.) Санкт-Петербург, 1998.
6. Гоголь А.А., Никодимов И.Ю. ОЧЕРКИ ИСТОРИИ РАЗВИТИЯ СВЯЗИ В РОССИИ Санкт-Петербург, 1999. Сер. «Телекоммуникации России: прошлое, настоящее, будущее».
7. Никодимов И.Ю., Морева В.Д. ИСПОЛЬЗОВАНИЕ МЕССЕНДЖЕРОВ ПРИ ПЛАНИРОВАНИИ ТЕРРОРИСТИЧЕСКИХ АКТОВ В сборнике: Проблемы назначения и исполнения наказания и мер уголовно-правового характера. Сборник статей. Под редакцией В.Ю. Голубовского. Москва, 2018. С. 63-67
8. Ильченко Е.А., Никодимов И.Ю. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В сборнике: УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ И НАКАЗАНИЕ.ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН. сборник статей по материалам научно-практической конференции. 2019. С. 77-85.
9. Никодимов И.Ю., Мансырев М.П., Пономарев С.П. ПЛАНИРОВАНИЕ СЕТИ GSM Электросвязь. 2000. № 3. С. 10
10. Никодимов И.Ю., Бучнев Д.Н. ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ И ПРАКТИКИ РЕГУЛИРОВАНИЯ ОПЕРАТОРСКОЙ ДЕЯТЕЛЬНОСТИ Мобильные системы. 1999. № 8. С. 11.
11. Гоголь А.А., Никодимов И.Ю. НОВЫЙ ЭТАП РАЗВИТИЯ ОТРАСЛИ СВЯЗИ: ЗАРОЖДЕНИЕ И РАЗВИТИЕ СОТОВОЙ СВЯЗИ Санкт-Петербург, 2000. Сер. Телекоммуникации России: прошлое, настоящее, будущее (2-е издание, исправленное и дополненное)

12. Никодимов И.Ю. СОВРЕМЕННЫЕ ПРОБЛЕМЫ ТЕОРИИ ИНФОРМАЦИОННОГО ПРАВА Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2016. № 2 (766). С. 105-117.