HACKER IN CUSTOMS SPHERE

Deryagin I.A. (Russian Federation) Email: Deryagin546@scientifictext.ru

Deryagin Ivan Aleksandrovich - Student-Master,
LEGAL DEPARTMENT,
ST. PETERSBURG BRANCH
RUSSIAN CUSTOMS ACADEMY NAMED AFTER V.B. BOBKOV, SAINT-PETERSBURG

Abstract: *the article analyzes the issues of information security of customs authorities, with the purpose of analyzing the current Russian legislation for compliance with the level of counteraction to the growing threat of computer crime in the Russian Federation and beyond. Hacking, as the most common and iconic type of crime in the field of computers crime, is subject to the most intensive study to counter it as a criminal phenomenons as a hacking, and, as a consequence, access to information materials.*
Keywords: *hacking, information protection, customs authorities.*

ХАКЕРСТВО В ТАМОЖЕННОЙ СФЕРЕ

Дерягин И.А. (Российская Федерация)

Дерягин Иван Александрович – студент-магистрант,
юридическая кафедра,
Санкт-Петербургский филиал
Российская таможенная академия им. В.Б. Бобкова, г. Санкт-Петербург

Аннотация: *в статье анализируются вопросы информационной безопасности таможенных органов, с целью анализа современного российского законодательства на соответствие уровню противодействия растущей угрозы компьютерной преступности в Российской Федерации и за её пределами. Хакерство, как наиболее распространённый и знаковый тип преступления в сфере компьютерной преступности, подлежит наиболее пристальному изучению для противодействия ему как преступному явлению, так как взлом, и, как следствие, получение доступа к информационным данным, служит первым и основным этапом в совершении преступления в сфере компьютерной информации.*
Ключевые слова: *хакерство, защита информации, таможенные органы.*

Возникновение и развитие компьютерной преступности неразрывно связаны с развитием использования компьютерных технологий.

Считается, что первое компьютерное преступление в 1969 г. совершил Альфонсе Конфессоре (США). Получив незаконно доступ к информации в электронно-вычислительной сети, он совершил налоговое преступление, ущерб от которого составил 620 тысяч долларов США.

На следующий год также путем незаконного доступа к информации «Секюрити пасифик бэнк» с одного из счетов банка было незаконно списано 10,2 миллиона долларов США.

Столкнувшись с компьютерной преступностью, органы уголовной юстиции зарубежных стран (а затем и России) начали борьбу с ней путем применения к виновным традиционных норм о хищениях или злоупотреблениях, но скоро поняли, что такой подход является неудачным.

Компьютерные преступления не укладываются в диспозиции норм об ответственности за названные преступления. В них не учтен способ совершения преступлений (использование высоких технологий), личность преступника и общественно опасные последствия, которые исчисляются миллиардами долларов США [5, с. 105]. Так возникли новые нормы уголовного права, предусматривающие ответственность за новый вид преступности (компьютерные преступления), которого не знало человечество на протяжении всего времени своего развития.

Первый законопроект, устанавливающий уголовную ответственность за преступления в сфере информационных технологий, был разработан в США еще в 1977 году. На основе данного законопроекта в октябре 1984 года был принят закон о мошенничестве и злоупотреблении с использованием компьютеров (Computer Fraud a№d Abuse Act, CFAA) - основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно дополнялся [3].

Закон о мошенничестве и злоупотреблении с использованием компьютеров 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.

Таким образом, информация, которой располагает таможенная служба, является основным объектом противоправного покушения.

Значимость и актуальность проблемы обеспечения информационной безопасности закреплена в списке приоритетных задач Таможенных органов и в Стратегии развития Таможенной службы до 2020 г. Именно п. 8 настоящей Стратегии включает в себя следующую задачу: «повышение уровня защищенности информационных ресурсов, расширение спектра мер по обеспечению информационной безопасности, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти [1].

Соответственно, перед обществом ставится проблема обеспечения информационной безопасности, что необходимо для устойчивого развития и благосостояния.

Таможенная служба не исключение. Она располагает огромными информационными ресурсами, которым также требуется защита. Но на таможенных органах лежит часть ответственности за национальную безопасность страны, поэтому надежное обеспечение информационной безопасности весомая часть достижения этой цели.

Условно обеспечение информационной безопасности таможенных органов можно разделить на два:

- это обеспечение информационной безопасности для цели обеспечения национальной безопасности (экономической, социальной, территориальной и т.д.);

- обеспечение информационной безопасности для целей своего нормального функционирования (эффективность управления, взаимодействия) [4, с. 6].

На основании этих направлений можно выделить виды информации, которые могут быть потенциальными объектами правонарушений.

Их можно условно разделить на внешние и внутренние виды информации.

Для их защиты существует особая институциональная система, которая структурирована в соответствии с институтами ФТС.

Угрозы обеспечения информационной безопасности таможенных органов реализуются возможными методами нарушения информационной безопасности. Таких методов среди экспертов называется пять.

Физические, радиоэлектронные, информационные, программно-математические и организационно

- правовые. Необходимо их разобрать по порядку.

1. Физические.

- Хищение и уничтожение средств связи, защиты и обработки информации. Умышленное нанесение на них неисправностей.

- Хищение и уничтожение носителей информации в электронном или ином виде.

- Хищение или уничтожение ключей, кодов доступа других средств от защиты несанкционированного доступа к информации.

- Физическое воздействие на пользователей и обслуживающий персонал системы ЕАИС в целях получения доступа к информации.

- Диверсии и теракты по отношению информационной инфраструктуре.

2. Радиоэлектронные

- Перехват информационных данных в сети интернет и линии связи.

- Перехват информационных данных в внутренних каналах ее утечки.

- Замена, навязывание ложных информационных данных в сети интернет и линий связи.

- Внедрение устройства – перехватчика данных.

- Подавление информационных данных путем различных генераторов электромагнитной энергии.

3. Информационные.

- Незаконный сбор, хранение, распространение и использование информации.

- Нарушение секретности информации.

- Противозаконное хранение, копирование, уничтожение информационных данных и программ.

- Различные манипуляционные действия с информацией (искажение информации, ее скрытие, дезинформация).

- Нарушение оперативности обмена информационными данными.

- Хищение информационных данных.

- Нарушение технологии информационного обмена и обработки информации.

4. Программно-математические.

- Создание и внедрение в информационную систему ЕАИС вредоносных программ (вирусов).

- Создание программ вирусов для компрометации системы защиты информации.

5. Организационно-правовые.

- Невыполнений законодательства в области обеспечения информационной безопасности таможенных органов РФ.

- Оборудование таможенных органов устаревшими и неактуальными средствами обеспечения информационной безопасности [2].

На сегодняшний день наиболее уязвимыми местами информационной безопасности таможенных органов России являются информационные угрозы. Связанно это с процессов и мировой глобализации, развитием НТП и недостаточным опытом борьбы с данным видом угроз.

Огромное количество угроз обеспечению информационной безопасности таможенных органов РФ делают данный процесс актуальным и приоритетным в работе Таможенных органов и правительства РФ.

Приведённая выше структура возможных угроз дает возможность прогнозировать возможные проблемы в определённых направлениях.

Определение факторов с сочетанием угроз дают нам возможность дальнейшего анализа в области обеспечения информационной безопасности.

Таким образом, с учетом всего вышесказанного, можно выделить пять основных методов правонарушения информационной безопасности таможенных органов, это физические, радиоэлектронные, информационные, программно-математические и организационно-правовые.

Данные методы являются основой для выделения основных видов Таможенных правонарушений в области информационной безопасности.

Список литературы

1. Распоряжение Правительства Российской Федерации от 28 декабря 2012 г. № 2575-р «Стратегия развития таможенной службы Российской Федерации до 2020 года».
2. *Барбышева Г.И., Мирзаев Ш.Ф.* Обеспечение информационной безопасности таможенных органов РФ [Текст] // Инновационная экономика: материалы II Междунар. науч. конф. (г. Казань, октябрь 2015 г.). Казань: Бук, 2015. С. 22-24.
3. Законодательство о киберпреступлениях в зарубежных странах. [Электронный ресурс]. Режим доступа: // https://ria.ru/spravka/20130809/955198703.html/ (дата обращения: 19.04.2018).
4. *Илюхина С.С.* Информационное обеспечение системы контроля корректировки таможенной стоимости товаров в аспекте реализации Стратегии развития таможенной службы России до 2020 года // Таможенное дело, 2015. № 2. С. 6-8.
5. Уголовное право. Особенная часть: Учебник для вузов / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. М., 1998. 768 с.