Новиков Михаил Юрьевич

Магистрант кафедры национального публичного и международного права юридического факультета РГСУ

Novikov Mikhail Yurievich
Master student of the Department of National public and international law Faculty of Law, RSSU

ИНСТРУМЕНТЫ ТЕХНИЧЕСКОЙ И ПРАВОВОЙ ЗАЩИТЫ ДОКУМЕНТОВ.

Instruments for technical and legal protection of documents

Аннотация: В современном мире высокими темпами развиваются такие направления в экономике как компьютеризация и телекоммуникация. Недостатком быстрого развития данных отраслей является задержка с компенсацией и ликвидацией различного рода побочных эффектов, возникающих при внедрении новшеств. Этим пользуются различного рода криминальные элементы и геополитические противники нашего государства. На ликвидацию юридических и технических пробелов, возникающих при внедрении современной техники направлена данная статья.

Ключевые слова: Юриспруденция в сфере высоких технологий, правовые аспекты компьютеризации, правовые аспекты инфокоммуникации, пробелы в законодательстве в сфере инфокоммуникации, кибер- атака.

Abstract: In the modern world, such directions in economics as computerization and telecommunications are developing at a high rate. The disadvantage of the rapid development of these industries is the delay in compensation and the elimination of various side effects arising from the

introduction of innovations. This is used by various kinds of criminal elements and geopolitical opponents of our state. This article is aimed at eliminating legal and technical gaps arising from the introduction of modern technology.

Keywords: jurisprudence in the field of high technologies, legal aspects of computerization, legal aspects of infocommunications, gaps in legislation in the sphere of infocommunications, cyber-attack.

С внедрением современных систем информатизации они оказались под пристальным прицелом различного рода преступных элементов. Так было всегда при внедрении любой техники, технологии или новой организации. Преступные элементы всегда проверяют возможность заработать вследствие недоработок в системе защиты. С другой стороны недобросовестные чиновники используя современные средства и системы инфокоммуникации недобросовестно выполняют свою работу, что сказывается негативно на гражданах Российской Федерации.[1]

Как можно систематизировать системы преступлений с использованием современной техники. Основной интерес у всех злоумышленников проявляется к той информации, которая находится на современных средствах и системах хранения и обработки информации а также в системах передачи информации.

Поэтому преступления в этой сфере можно разделить на три элемента

1. Хищение информации с помощью современных средств хранения, обработки и передачи информации.
2. Модификация информации с помощью современных средств хранения, обработки и передачи информации.

[1]Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Владивосток, 2007. С. 5

3. Уничтожение информации с помощью вывода из строя аппаратных или программных средств хранения, обработки и передачи информации.

Злоупотребление со стороны чиновников можно отнести к разновидности модификации информации с помощью современных средств хранения, обработки и передачи информации. Оно заключается в использовании современных систем обработки информации в таких операциях как коммунальные платежи, начисление налогов, работа судебных приставов, запись в поликлинику и др. В последнее время после внедрения современных средств обработки информации в данные операции привели к усложнению и , главное , к отдалению граждан Российской Федерации от государства. Если раньше гражданин сталкивался с интересами государства через его чиновника и имел визуальный и вербальный контакт с ним, что значительно усложняло злоупотребление со стороны чиновника с одной стороны. То в настоящий момент граждане получают распечатки на коммунальные платежи, решения суда, начисление налогов, запись в поликлинику через дополнительную бюрократическую структуру – машино-аппаратный комплекс. Создана дополнительная бюрократическая прослойка, которая ни за что не отвечает. Не правильно начислены коммунальные платежи – спрашивать не с кого, не правильно рассчитан налог – спрашивать не с кого и так далее. Все это способствует злоупотреблению чиновничьего аппарата и вместе с тем способствует росту социальной напряженности. К сожалению данный вопрос до сих пор не решен. А необходимо упростить систему обращения с исками на злоупотребления чиновников. Если у чиновников есть машино-аппаратный комплекс - такой-же должен быть и у граждан.[2]

Теперь рассмотрим преступления.

---

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 17.06.1996. N 25. Ст. 2954

К первому типу преступлений относится хищение информации. Основная часть всей информации хранится в виде документов.

Всю историю человечества документы играли важную роль в жизни человека и общества. Человек приходя в этот мир первым делом получает документ, свидетельствующий об этом, документы сопровождают его всю жизнь вплоть до самых последних дней.[3]

С развитием общества, документов различного характера становилось всё больше, появилось множество различных уровней конфиденциальности документа. Наибольшая активность по генерации документов конечно же наблюдается в крупных корпорациях. Тонны документов хранятся в архивах компаний, государственных архивах. С развитием компьютерных технологий появилась возможность создавать электронные копии документов и хранить их в электронных базах данных. В этом есть как положительные, так и отрицательные стороны. В первую очередь, отсканированный документ может храниться в любой точке планеты, в любом помещении, так как для него отсутствует необходимость создавать условия хранения, как для документа на физическом носителе. Имеется ввиду определённая температура, влажность воздуха, комплекс мер по обеспечению безопасности при пожаре и стихийных бедствиях. Но электронный документ уязвим для разного рода компьютерных мошенников, людей или группы лиц, целью которых является хищение конфиденциальных документов. В дальнейшем документы либо продают, либо на основании полученной информации шантажируют собственников документа или просто публикуют документ в сети интернет для публичного доступа.

---

[3] ст. 159.6 УК РФ ("Мошенничество в сфере компьютерной информации"), введена в действие Федеральным законом от 29.11.2012 N 207-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" // Российская газета. N 278. 03.12.2012.

Для электронных баз данных документов есть свои требования для хранения и обеспечения их безопасности. Конечно, одним из самых простых способов защиты документов от кибер-атак является отсутствие подключения к сети интернет ЭВМ на которых хранятся БД электронных документов. Но в таком случае возникает и следующий вопрос, каким образом пополнять БД новыми документами? Скорее всего, будет предложено загружать новые документы посредством флэш накопителей (флешки, переносные жёсткие диски и т.д.) через usb порт. В таком случае на компьютер может быть занесена вирусная программа, целей и задач у которой тоже может быть множество. От полного уничтожения БД до выведения из строя ЭВМ.[4]

Выделим три реальных метода защиты от угроз со стороны USB-накопителей:

- программно-аппаратные средства защиты от несанкционированного доступа (СЗИ НСД);
- DLP-системы;
- пофайловое или посекторное ("прозрачное") шифрование данных на USB-носителе.

В конечном итоге избавиться от остаточного риска можно используя аппаратные решения: специализированные USB-носители.

Вопрос о создании БД, обеспечения безопасности БД и при этом доступности информации в них достаточно широк. Но как показывает статистика, больший риск возможности утечки конфиденциальных документов это не преднамеренное действия сотрудников с низким уровнем знаний по работе и обеспечению безопасности электронных БД. Данная статья позволит освоить первую ступень.

Ко второму типу преступлений относят модификацию информации. Под модификацией понимают намеренное изменение или искажение

[4] Combating computer crime. Prevention. Detection. Investigation / Chantico publishing company, inc. 1990.

информации без согласия или уведомления ее правообладателя. Данный вид преступлений встречается реже чем первый, однако является более изощренным и не менее опасным, чем простое хищение. Ведь при модификации информации злоумышленник ставит задачу не столько личного обогащения сколько нанесения ущерба собственнику информации.[5]

К третьему типу преступлений относят уничтожение информации. Уничтожение информации осуществляется либо с помощь физического уничтожения или вывода из строя ПЭВМ либо ее компонентов, а также различного рода носителей информации (магнитные носители, диски, флешки и прочие электронные «накопители»).

И если технические способы защиты были рассмотрены при обсуждении первого типа преступлений, то юридические способы защиты рассмотрим ниже:

Впервые вопросы регулирования хранения и защиты информации были рассмотрены в Законе от 23.09.1992г. « О правовой охране программ для электронно-вычислительных машин и баз данных». Затем Закон от 20.02.1995г. « Об информации, информатизации и защите информации» , затем Закон от 10.01.2002г. «Об электронной цифровой подписи».

Однако основные вопросы защиты информации в настоящий момент отражены в Главе 28 УК РФ.

Основное, что было предпринято для избегания хищения, модификации и уничтожения информации это юридическая защита от доступа сторонних лиц к данной информации без санкции правообладателя. Эта идея изложена в ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Объективная сторона данного преступления состоит в

---

[5] Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше)// Вестник ТГПУ. Серия "Гуманитарные науки (юриспруденция)". 2006. N 11

неправомерном доступе к охраняемой законом компьютерной информации (Информации, находящейся на ЭВМ, машинном носителе, магнитном носителе, в сети ЭВМ или во время передачи информации по проводной или беспроводной сети).

С одной стороны такая форма защиты , казалось бы, должна предотвратить мошенничество в сфера высоких технологий. Однако в статье закона говорится об охраняемой законом информации. А что значит охраняемая законом информация? Под данной категорией подразумевается следующее:

· информация, составляющую государственную тайну, режим защиты которой устанавливается федеральным законом;

· конфиденциальная информация, режим защиты которой устанавливается в основном собственником или владельцем на основании закона, а в ряде случаев федеральным законом;

· документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты устанавливается собственником или владельцем на основании закона.

С другой стороны вопрос охраняемой законом информации до сих пор не урегулирован. Иначе как можно понимать судебную практику, которая признавала нарушением статьи 272 проникновение в любую информацию, находящуюся на машинном носителе. Данный вопрос требует дальнейшей проработке.

Список литературы.

1. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Владивосток, 2007. С. 5

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 17.06.1996. N 25. Ст. 2954
3. ст. 159.6 УК РФ ("Мошенничество в сфере компьютерной информации"), введена в действие Федеральным законом от 29.11.2012 N 207-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" // Российская газета. N 278. 03.12.2012.
4. Combating computer crime. Prevention. Detection. Investigation / Chantico publishing company, inc. 1990.
5. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше)// Вестник ТГПУ. Серия "Гуманитарные науки (юриспруденция)". 2006. N 11
6. Никодимов И.Ю АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА. Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2016. № 1 (763). С. 147-160.
7. 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.
8. 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.

9. Никодимов И.Ю. НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДМЕТА ИНФОРМАЦИОННОГО ПРАВА Правовое поле современной экономики. 2015. № 12. С. 135-140.
10. Гоголь А.А., Никодимов И.Ю. СТРАНИЦЫ ИСТОРИИ РАДИОСВЯЗИ (КОНЕЦ XIX – ПЕРВАЯ ЧЕТВЕРТЬ XX В.) Санкт-Петербург, 1998.