**7. Преступления в сфере компьютерной информации**

***Понятие преступления в сфере компьютерной информации. Классификация преступлений в сфере компьютерной безопасности. Состав преступлений в сфере компьютерной безопасности. Нормативно-правовое регулирование преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.***

**7.1. Понятие преступления в сфере компьютерной информации.**

Под **компьютерными преступлениями** понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

В литературе преступления в сфере компьютерной информации иногда отождествляют с компьютерными преступлениями, но бывает и такое, особенно, когда это касается классификации преступлений – преступления в сфере компьютерной информации рассматриваются в качестве одной из групп компьютерных преступлений.

Тем самым налицо два варианта соотношения категорий «преступления в сфере компьютерной информации» и «компьютерные преступления»:

в первом – эти категории рассматриваются как тождественные;

во втором – первая категория является частью второй.

Из этого следует, что компьютерные преступления можно рассматривать в двух значениях: в узком как в первом случае и широком как во втором случае.

В нашем случае, чтобы не путаться будем использовать законодательную формулировку – «преступления в сфере компьютерной информации».

Что же следует понимать под понятием «преступления в сфере компьютерной информации»?

Для ответа на данный вопрос как минимум необходимо учитывать, что, данные преступления, предусмотрены *главой 28 УК РФ Раздела IX УК РФ* и они посягают на компьютерную информацию.

Под **компьютерной информацией**, согласно примечания *1 к ст. 272 УК РФ*, понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Таким образом, под **преступлениями в сфере компьютерной информации** можно понимать общественно опасные деяния, предусмотренные *главой 28 раздела IX УК РФ*, посягающие на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В литературе встречается несколько определений данного вида преступления.

– общественно опасные посягательства на общественную безопасность, запрещённые уголовным законом под угрозой наказания и совершённые в области информационных правоотношений;

– запрещенные уголовным законом виновные посягательства на безопасность в сфере использования компьютерной информации, причинившие существенный вред или создавшие угрозу причинения такого вреда личности, обществу или государству;

– виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания;

– общественно опасные деяния, ответственность за которые предусмотрена ст. 272-274 г. 28 раздела 9 УК РФ, посягающие на  общественные отношения, обеспечивающие права и законные интересы граждан и организаций, охраняемые законом  интересы общества и государства в сфере создания и обращения компьютерной информации;

– виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания;

– общественно опасные противоправные деяния, которые имеют своим дополнительным родовым объектом общественные отношения по обеспечению информационной безопасности общества, посягающие на нормальный режим хранения, обработки и передачи данных в компьютерах (компьютерных системах);

– предусмотренные *ст. 272-274 гл. 28 УК* умышленные или неосторожные общественно опасные деяния (действия или бездействие), направленные против безопасности компьютерной информации и причиняющие либо способные причинить вред охраняемым законом благам (отношениям собственности, правам личности и т.д.).

**7.2. Классификация преступлений в сфере компьютерной** безопасности.

В марте 2001 года был представлен доклад Комиссии по предупреждению преступности и уголовному правосудию ООН, в котором все компьютерные преступления были классифицированы следующим образом:

1) **преступления, совершаемые против технологий и их пользователей**, – несанкционированный доступ к компьютерам или информационным системам; несанкционированное использование информационных систем; несанкционированное прочитывание, копирование и использование данных; создание и распространение вредоносных программ; компьютерный вандализм или саботаж;

2) **традиционные преступления, совершаемые с использованием компьютерных или коммуникационных технологий**, – преступления, связанные с информацией незаконного содержания; похищение человека с использованием сети Интернет; мошенничество; коммерческий или промышленный шпионаж; преступления, связанные с нарушением прав интеллектуальной собственности; игорный бизнес; легализация средств, полученных преступным путем;

3) использование компьютерных технологий для поддержки другой преступной деятельности.

В зависимости от объекта и предмета посягательства все компьютерные преступления, предусмотренные как в российском, так и зарубежном уголовном праве, можно разделить на две группы:

1. Преступления в сфере компьютерной информации. Предметом в таких преступлениях выступает компьютерная информация, как, например, в деяниях, предусмотренных *статьями 272-274 УК РФ*, статьями 361-363 УК Украины, §1030 (а)(1) Свода Законов США «Несанкционированный доступ к информации с ограниченным доступом, касающейся национальной безопасности, международных отношений, атомной энергетики», статьей 478.1 УК Австралии «Несанкционированный доступ или модификация охраняемой компьютерной информации или программы» и рядом других.

2. Преступления, где компьютерная информация является орудием или средством совершения другого преступления. Эти составы преступлений находятся в других главах уголовных кодексов, к примеру, в статье 212 УК Республики Беларусь «Хищение путем использования компьютерной техники»; §1030(а)(7) Свода Законов США «Вымогательство, угрозы причинения вреда с использованием компьютера»; статье 206(1)(е) УК Канады «Использование компьютерных данных и технологий в целях извлечения прибыли путем создания финансовых пирамид» и других. Применительно к УК РФ, ответственность за преступления этой группы должна наступать по иным статьям Кодекса в соответствии с их родовым и непосредственным объектами. Однако такие деяния в необходимых случаях могут квалифицироваться по совокупности с преступлениями, предусмотренными *статьями 272-274 УК РФ*.

В литературе встречается мнение, что «Гражданский кодекс РФ (*Часть IV ГК РФ*) содержит перечень конкретных объектов правовой охраны, подпадающих под понятие интеллектуальной собственности, включая программы для ЭВМ. В связи с этим необходимо отнесении к числу преступлений против интеллектуальной собственности  так называемые компьютерные преступления – (*ст.ст. 272, 273, 274 УК РФ*)».

Действительно, с точки зрения гражданского законодательства программы для ЭВМ являются одним из объектов интеллектуальной собственности (*п. 2 ч.1 ст. 1225 ГК РФ)*, но также они относятся к объектам авторских прав, которые охраняются как литературные произведения (*абз. 2 ч. 1 ст. 1259 ГК РФ*). Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы (*ст. 1261 ГК РФ*).

Итак, программы для ЭВМ являются одним из объектов интеллектуальной собственности, на них существуют авторские права и они охраняются так же, как авторские права на произведения литературы.

В уголовном праве авторские права находятся под охраной *ст. 146 УК РФ* «Нарушение авторских и смежных прав».

Следовательно, к преступлениям против интеллектуальной собственности нельзя отнести так называемые компьютерные преступления – (*ст.ст. 272, 273, 274 УК РФ*).

**7.3. Состав преступлений в сфере компьютерной безопасности.**

**Предмет преступления**– охраняемая законом компьютерная информация, которая находится на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

**Предмет преступлений** в сфере компьютерной информации – это компьютерная информация, то есть сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

**Видовым объектом** Главы 28 УК РФ являются общественные отношения в сфере обеспечения нормального оборота компьютерной информации.

**Непосредственный объект**– общественные отношения в сфере компьютерной информации, например неправомерный доступ к компьютерной информации (*ст. 272 УК РФ*).

**Объективная сторона**– неправомерный доступ к указанной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

**Объективная сторона** преступлений, предусмотренных *ст.ст. 272-274 УК РФ*,  может характеризоваться деянием как в форме действия: неправомерный доступ к компьютерной информации (*ст.  272*), создание, использование и распространение вредоносных компьютерных программ (*ст. 273*), так и в форме как действия или бездействия – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (*ст. 274*).

По конструкции объективной стороны два из трёх составов преступлений в сфере компьютерной информации являются материальными, то есть предполагающими наличие деяния и наступления указанных в уголовном законе общественно опасных последствий: по *ст. 272 УК РФ* в виде уничтожения, блокирования, модификации либо копирования компьютерной информации; по *ст. 274 УК РФ* в виде крупного ущерба, и, безусловно, наличия причинной связи между деянием и последствиями.

Виды неправомерных деяний.

**Незаконный доступ** означает, что у лица, осуществляющего сбор, обработку, поиск и т. п., нет права на осуществление такой деятельности. Способы совершения могут быть различными – использование чужого пароля, кода, чужого имени, хищение носителей информации и т. п.

**Уничтожение информации**– удаление ее полностью или частично из ЭВМ, с материальных носителей.

**Блокирование информации**– совершение действий, в результате которых возникает невозможность дальнейшего использования компьютерной информации.

**Модификация**– это любые изменения компьютерной информации, за исключением изменений, осуществляемых исключительно в целях обеспечения функционирования ЭВМ, программ для ЭВМ или баз данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

**Копирование**– воспроизведение информации на другом материальном носителе при сохранении неизмененной первоначальной информации.

**Объективная сторона** *ст. 273 УК РФ* заключается в следующих альтернативных действиях:

– создание программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

– внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

– использование таких программ или машинных носителей с такими программами;

– распространение таких программ или машинных носителей с такими программами.

**Объективная сторона** *ст. 274 УК РФ* выражается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшем уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, при условии, что это деяние причинило существенный вред.

**Субъективная сторона** *ст. 272 УК РФ* характеризуется виной в форме умысла как прямого, так и косвенного; *ст. 273 УК РФ* – только прямым умыслом; ст. 274 УК РФ – как умышленной, так и неосторожной виной.

**Субъект компьютерных преступлений** (*ст.ст. 272-273 УК РФ*) общий – физическое, вменяемое лицо, достигшее шестнадцати лет.

**Специальный субъект преступления**, предусмотрен как *ч. 3 ст. 272 УК РФ*, так и *ч.2 ст. 273 УК РФ* – это «лицо, использующее свое служебное положение», а также *ст. 274 УК РФ* – это лицо обязанное соблюдать  правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правила доступа к информационно-телекоммуникационным сетям.

**7.4. Нормативно-правовое регулирование преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.**

Конституция РФ, с одной стороны, провозгласила, что: каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (*ч. 4 ст. 29*), а с другой – установила, что: каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ч.2 ст. 23); Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (*ч.1 ст. 24*).

Таким образом, Конституция РФ не только предоставляет право на информацию, но и гарантирует её защиту.

В России действует Федеральный закон *от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»*, где в *ч. 1 ст. 16*  указывается, что: Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Одной из мер правового характера по обеспечению защиты информации является *Глава 28 УК РФ* «Преступления в сфере компьютерной информации».

Роль и место преступлений в сфере компьютерной информации, предусмотренных *Главой 28 УК РФ*, в системе преступлений против общественной безопасности и общественного порядка  *Раздела IX УК РФ* определяется тем, что:

а) *Раздел IX УК РФ* заканчивается именно  этой – пятой по счёту в *Разделе IX УК РФ главой – главой 28 УК РФ* «Преступления в сфере компьютерной информации»;

б) в этой Главе самое маленькое количество статей из всех Глав *Раздела IX УК РФ. Глава 28 УК РФ* «Преступления в сфере компьютерной информации» состоит из 3 статей (*ст. 272-274 УК*):  неправомерный доступ к компьютерной информации (*ст. 272*); создание, использование и распространение вредоносных компьютерных программ (*ст. 273*); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (*ст. 274);*

в) в этой Главе нет преступлений за которые, согласно *ч.2 ст. 20 УК РФ*,  уголовная ответственность бы наступала с 14 лет.

г) это совершенно новая глава и преступления в ней неизвестные до УК РФ 1996 года уголовному законодательству.

Понятие **единичного преступления в сфере компьютерной информации** даётся в ратифицированном *Федеральным законом РФ от 1 октября 2008 года N 164-ФЗ* «[Соглашени](consultantplus://offline/main?base=INT;n=9210;fld=134)и о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации  (Минске 1 июня 2001 года)».

Согласно *п. «а» ст. 1 этого Соглашения*: **преступление в сфере компьютерной информации** – уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация.

При сравнении положений УК РФ и Модельного Уголовного кодекса стран СНГ в вопросе преступлений против компьютерной информации, получим следующую картину:

во-первых, если в *УК РФ Глава 28* «Преступления в сфере компьютерной информации»  является только одной из глав *Раздела IX УК РФ* «Преступлений против общественной безопасности и общественного порядка», то в *Модельном Уголовном кодексе стран СНГ Глава 30* «Преступления против информационной безопасности», является единственной главой в одноимённом разделе – *Разделе XII «Преступления против информационной безопасности»*;

во-вторых, если *28 Глава  УК РФ* называется «Преступления в сфере компьютерной информации», то в *Модельном Уголовном кодексе стран СНГ Глава 30* носит название «Преступления против информационной безопасности»;

в-третьих, если *Глава 28 УК РФ* содерж*ит три преступления, то* Глава 30 Модельного Уголовного кодекса стран СНГ шесть преступлений, причём три из которых – это: несанкционированный доступ к компьютерной информации (*ст. 286*); разработка, использование и распространение вредоносных программ (*ст. 291*); нарушение правил эксплуатации компьютерной системы или сети (*ст. 292*) в целом совпадают со всеми тремя преступлениями *Главы 28 УК РФ* – это: неправомерный доступ к компьютерной информации (*ст. 272*), создание, использование и распространение вредоносных компьютерных программ (*ст. 273*), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (*ст.  274*).

Соответственно, остальные три преступления, предусмотренные *Главой 30 Модельного Уголовного кодекса стран СНГ* – это: компьютерный саботаж (*ст. 288*); неправомерное завладение компьютерной информацией (*ст. 289*); изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (*ст. 290*) не находят своего места в *Главе 28 УК РФ «Преступления в сфере компьютерной информации»*.

**Рекомендуемая литература:**

1. Кудрявцев В.Л.  Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка. Материалы международной научно-практической конференции (Нижний Новгород, 1 марта 2012 года) / Под ред.: Козлов А.В., Панченко П.Н. – Нижний Новгород: НИУ ВШЭ – Нижний Новгород, 2012. С. 69–76. – Режим доступа: <http://www.iuaj.net/node/1174>.

2. Модельный Уголовный кодекс: Рекомендательный законодательный акт для Содружества Независимых Государств, Принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств ([постановление N 7-5 от 17 февраля 1996 года](постановление%20N%207-5%20от%2017%20февраля%201996%20года)). – Режим доступа: <http://docs.cntd.ru/document/901781490>.

3. Нормативно-правовые акты, указанные в тексте.

**Контрольные вопросы:**

1. Что понимается под компьютерными преступлениями?

2. Сравните понятия «преступления в сфере компьютерной информации» и «компьютерные преступления».

3. Что же следует понимать под понятием «преступления в сфере компьютерной информации»?

4. Что понимается под **компьютерной информацией**?

5. Сравните различные варианты определений понятия «преступление в сфере компьютерной информации».

6. Назовите основания для классификации в сфере компьютерной информации.

7. Что является предметом преступления?

8. Что является объективной стороной преступления в сфере компьютерной безопасности?

9. Назовите виды неправомерных деяний в сфере компьютерной безопасности.

10. Что означает незаконный доступ к информации?

11. Что означаетуничтожение информации?

12. Что означает блокирование информации?

13. Что означает модификация информации?

14. Что означает копирование информации?

15. Опишите состав ст. 272 УК РФ.

16. Опишите состав ст. 273УК РФ.

17. Опишите состав ст. 274 УК РФ.