ГЛАВА XI.

ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ И ПРЕСТУПЛЕНИЯ В ОБЛАСТИ ЭЛЕКТРОСВЯЗИ

[Название в редакции Закона № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]
[Название в редакции Закона №№254-XV от 09.07.2004 г., в силу с 22.10.2004 г.]

Статья 259. Несанкционированный доступ к компьютерной информации

(1) Неправомерный доступ к компьютерной информации, то есть к информации в компьютерах, на машинных носителях, в информационной системе или сети, лица, не имеющего такого права в силу закона или договора, превышающего пределы разрешения или не получившего разрешение лица, правомочного использовать, администрировать или контролировать информационную систему либо проводить научные исследования или производить иного рода операции в информационной системе, сопряженный с уничтожением, повреждением, модификацией, блокированием или копированием информации, нарушением работы компьютеров, информационной системы или сети и повлекший причинение ущерба в крупных размерах, наказывается штрафом в размере от 200 до 500 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 150 до 200 часов, или лишением свободы на срок до 2 лет, а в случае юридического лица — штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

(2) То же действие, совершенное:

[Пкт. a) исключен Законом № 277-XVI от 18.12.2008 г., в силу с 24.05.2009 г.]

b) двумя или более лицами;
c) с нарушением систем защиты;
d) путем подключения к каналам связи;
e) с использованием специальных технических средств;
f) с неправомерным использованием компьютера, информационной системы или сети для совершения одного из преступлений, предусмотренных частью (1), статьями 2601-2603, 2605 и 2606;
g) в отношении охраняемой законом информации;
h) в особо крупных размерах, наказывается штрафом в размере от

500 до 1000 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 180 до 240 часов, или лишением свободы на срок до 3-х лет, а юридическое лицо наказывается штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или с ликвидацией юридического лица.

[Ст. 259 изменена Законом № 277-XVI от 18.12.2008 г., в силу с 24.05.2009 г.]
[Ст. 259 изменена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]
[Ст. 259 изменена Законом № 184-XVI от 29.06.2006 г., в силу с 11.08.2006 г.]
[Ст. 259 дополнена Законом № 211-XV от 29.05.2003 г., в силу с 12.06.2003 г.]

1. Опасность компьютерных преступлений состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем оборонного, безопасности и производственного назначения, способны повлечь гибель людей, причинить вред их здоровью, нанести ущерб государственной безопасности и общественному порядку, уничтожить имущество в больших размерах. Придавая большую значимость и важность данным явлениям мировое сообщество в самом конце прошлого столетия приняла международную Конституцию "Международный Союз телефонных сообщений" (1999 год), а в начале XXI века приняло Международную Конвенцию "О преступности в сфере информатики" (2001 год). Вслед за вышеназванными международными правоприменительными актами мировым сообществом 29.06.2004 г. была принята международная Конвенция "О международном Союзе телефонных сообщений".

Учитывая эти обстоятельства, законодатель Республики Молдова отнес гл. XI Уголовного кодекса Республики Молдова к "Преступлениям в области информатики и электросвязи".

В Республике Молдова на законодательном уровне отношения в сфере электрической связи и компьютерной информации урегулированы законами: "Об электрической связи" (1995 год), "Об информатике" (2001 год), "Об информатизации и государственных информационных ресурсах" (2003 год) "Об электронной торговли" (2004 год).

Компьютерная информация имеет специфику, которую на наш взгляд нужно свести к следующим критериям:

1) данная информация, как правило, очень объемна и быстро обрабатываема;

2) эта информация очень легко и в основном бесследно уничтожаема;

3) компьютерная информация обезличена, то есть между ней и лицом, которому она принадлежит, нет взаимной обусловленной жесткой связи, которая подтвердила бы право собственности на нее;

4) данный вид информации может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и других носителях), в самой ЭВМ (оперативной памяти);

5) рассматриваемый вид информации может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВМ при наличии соответствующих периферийных устройств чтения машинных носителей информации (дисководы, устройства чтения лазерных дисков (CD-ROM), стримеры, устройства чтения цифровых видеодисков и др.);

6) эта информация легко передается по телекоммуникационным каналам связи компьютерных сетей, причем ее полный объем можно передавать на любое расстояние Земного шара;

7) эта информация при изъятии, в отличие от вещи, легко сохраняется в первоисточнике и доступ к одному и тому же файлу, содержащему информацию могут иметь одновременно несколько пользователей.

Компьютерная информация, которую также можно определить и как информацию, зафиксированную на машинном носителе или передаваемую по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

Непосредственно информация на сегодняшний день не является предметом, какой либо гражданской сделки и не предназначена для купли-продажи. Компьютерная информация является только предметом авторского права, в некоторых случаях очень трудно определить ее истинного автора.

Уголовное законодательство охраняет далеко не всю информацию, а лишь ту, которая имеет научное, практическое юридическое значение. Изучение преступлений, предусмотренных гл. XI УК РМ, во многом обусловлено уяснением терминов, взятых из технических наук, которые используются законодателем, учеными-криминалистами, криминологами, а также практическими работниками правоохранительных органов.

База данных — поименная совокупность структурированных данных, относящихся к определенной предметной области.

Базовый компьютер — основной тип компьютера, используемый в большой информационной сети.

Безбумажная информация — технология сбора, накопления, переработки и обмена или распространения информации на основе ЭВМ и машинных носителей: магнитных лент, дисков и т.п.

Вычислительная техника — совокупность технических и материальных средств (электронно-вычислительные машины (ЭВМ), устройства, приборы, программы и др.), предназначенных и используемых для автоматизации процессов обработки информации.

Данные — информация, представленная в формализованном виде, пригодном для введения ее в ЭВМ и последующей автоматизированной обработки.

Запоминающее устройство (устройство памяти) — часть ЭВМ, выполняющая функции памяти. Основными характеристиками являются: емкость, методы доступа, надежность работы, стоимость.

Информационная безопасность личности, общества и государства —

состояние защищенности всех субъектов общественных отношений от вредной или непроверенной информации (дезинформации).

Информационные ресурсы — массивы документальной информации в информационных системах (библиотеках, архивах, фондах, банках данных). Информационные ресурсы образуют основу для развития процесса информатизации общества.

Информация — совокупность данных, сведений, фактов, циркулирующих в информационных процессах, в каналах прямой и обратной связи.

Компьютерный вирус — программа, способная разрушить программы, находящиеся в памяти других компьютеров и целых компьютерных систем, а также привести к сбоям в работе компьютера или компьютерной сети либо самопроизвольно копировать себя с компьютера на компьютер.

Международная информационная сеть — такая информационная компьютерная сеть, компоненты которой расположены в разных странах.

Программа — последовательность указаний (команд) для ввода исходных данных, их обработки и выдачи результатов для реализации алгоритма задачи.

Программа управляющая — системная программа для управления работой компьютера или вычислительной системой, т.е. для обеспечения взаимосвязанного функционирования всех устройств ЭВМ при обработке заданий.

Программирование — процесс описания алгоритма решения задачи средствами конкретного языка программирования и оформления результатов описания в виде программы.

Система ЭВМ — ряд программно-совместимых ЭВМ, имеющих одинаковую архитектуру (совокупность основных устройств, узлов и блоков ЭВМ). Система ЭВМ образует компьютерную (вычислительную, информационную) сеть.

Электронная вычислительная машина (компьютер) — комплекс технических средств, предназначенных для автоматической обработки информации в решении вычислительных и информационных задач.

Файл — совокупность упорядоченных и взаимосвязанных записей данных.

2. Уголовный закон не дает определения несанкционированному доступу к охраняемой законом компьютерной информации. Законодатель раскрывает лишь его последствия, которые повлекли за собой уничтожение, повреждение, модификацию, блокирование или копирование информации, а также незаконные действия, в результате которых была нарушена нормальная работа компьютера (компьютеров), компьютерных систем или компьютерных сетей.

Непосредственным объектом анализируемого преступления являются общественные отношения, по обеспечению безопасности компьютерной информации и нормальной работы электронно-вычислительных машин (ЭВМ), систем ЭВМ или их сети.

Дополнительный объект несанкционированного доступа к компьютерной информации факультативен. Его наличие и определение зависит от вида вреда,

причиненного правам и законным интересам потерпевшего. Так, например, по нашему мнению, в качестве дополнительного объекта может выступать, право собственности, авторское право, право на неприкосновенность частной жизни, личную и семейную тайну, общественные отношения по охране окружающей среды, внешняя безопасность государства и другие общественные отношения.

Предметом преступного посягательства является охраняемая законом компьютерная информация, которая с позиции уголовно-правовых норм характеризуется следующими обязательными признаками:

a) она всегда является интеллектуальной собственностью;

b) она не обладает натуральными физическими параметрами, то есть она не может восприниматься как вещь;

c) она охраняется законом;

d) она содержится на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Предметом данного преступления является та компьютерная информация, которая находится на машинных носителях в электронно-вычислительной машине (ЭВМ) в системе ЭВМ или в их сетях и которая регулируется законодательством об авторском праве, о праве собственности, о частной жизни человека, о тайне следствия и судопроизводства, о служебной, профессиональной, коммерческой тайне.

По смыслу диспозиции ч. (1) ст. 259 УК РМ неправомерный доступ к компьютерной информации образует состав преступления, если она задокументированна:

- на машинных носителях — CD-ROM, дискетах, перфокартах, схемах, подлежащих расшифровке с использованием программ для ЭВМ;
- в электронно-вычислительной машине — техническом средстве, предназначенном для автоматической обработки компьютерной информации;
- в системе ЭВМ — объединении взаимодействующих процессоров, периферийного оборудования и программного обеспечения, предназначенной для автоматизации хранения, обработки и выдачи информации пользователям;
- в сети ЭВМ — объединении нескольких ЭВМ, предназначенной для коллективного использования сетевых ресурсов (локальные сети достаточно широко используются в организациях для интенсификации деятельности).

Законодатель предусмотрел уголовную ответственность по ст. 259 УК РМ за неправомерный доступ к информации, лишь, если она запечатлена на машинном носителе, в ЭВМ, системе или сети ЭВМ и если в результате этого незаконного доступа была уничтожена, повреждена, модифицирована, блокирована или копирована информация, либо нарушена работа компьютеров, компьютерных систем или компьютерных сетей. Компьютерная информация содержащаяся в памяти ЭВМ реализуется через материальные носители, в качестве которых выступают: дискета, магнитные ленты, аппаратно-техническая

часть и программное обеспечение ЭВМ. Компьютерная информация, где бы она ни содержалась и ни циркулировала (в памяти ЭВМ, в каналах связи, на магнитных носителях), охраняется уголовным законом.

3. *Объективная сторона* рассматриваемого преступления, предусмотренного ч. (1) ст. 259 УК РМ, характеризуется действиями, то есть осуществлением неправомерного доступа виновного к компьютерной информации или информационным ресурсам (массивам документальной информации в информационных системах) на любой стадии технологического процесса обработки информации с использованием ЭВМ, системы или сети ЭВМ: при сборе данных и переносе их на машинные носители; при формировании и вводе массива информации в память ЭВМ; при передаче информации по каналам связи, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или сети ЭВМ.

Исходя из определения законодателя, становится возможным выделить три обязательных признака несанкционированного доступа к компьютерной информации, характеризующие данный состав преступления с объективной стороны:

- *общественно опасное деяние,* к которому законодатель относит несанкционированный доступ к охраняемой законом компьютерной информации;
- *общественно опасные последствия* в виде уничтожения, повреждения модификации, блокирования или копирования компьютерной информации, нарушения работы компьютеров, компьютерных систем или их сетей;
- *причинная связь между совершенным деянием и наступившими последствиями.*

Отсутствие хотя бы одного из перечисленных признаков означает и отсутствие самого состава преступления и соответственно уголовной ответственности, предусмотренного по ст. 259 УК РМ.

К объективным признакам исследуемого состава преступления относится общественно опасное деяние, которое всегда проявляется в активной форме поведения виновного. Совершить несанкционированный доступ к компьютерной информации путем бездействия как теоретически, так и практически не представляется возможным.

Одним из необходимых оснований для привлечения виновного к уголовной ответственности по ст. 259 УК РМ является установление факта несанкционированного действия, когда виновное лицо не имело *разрешения на вызов* информации хранящейся в компьютерах или на машинных носителях, знакомство с ней и распоряжение ею по своему усмотрению. Из диспозиции данной нормы исходит, что лицо для того чтобы вызывать информацию должно иметь на это официальное *разрешение* или *согласие* в письменном виде от владельца ЭВМ, компьютера, компьютерной системы или их сетей. Согласно действующему Гражданскому Процессуальному кодексу РМ разрешение или

согласие на какие-либо действия дается только в письменной форме. Устная форма законодательством не предусмотрена. Таким образом, *несанкционированный доступ к компьютерной информации* является первым и обязательным признаком, характеризующим рассматриваемое преступление с объективной стороны.

Вторым обязательным признаком объективной стороны несанкционированного доступа к компьютерной информации является общественно опасное последствие, сопряженное с уничтожением, повреждением, модификацией, блокированием или копированием информации, нарушением работы компьютеров, компьютерных систем или их сетей. Ознакомление с информацией, хранящейся в памяти компьютера, не позволяет привлечь лицо к уголовной ответственности по ст. 259 УК РМ, если не наступили указанные в законе последствия.

Причиняя ущерб компьютерной информации путем ее уничтожения, блокирования, модификации и т.д., виновный тем самым причиняет ущерб ее владельцу. Между наступлением указанных последствий и неправомерным доступом к компьютерной информации должна быть установлена причинная связь.

Под *уничтожением информации* следует понимать полное или частичное удаление ее с машинных носителей, что обусловливает утрату ее качественных признаков, ее сущности. Имеющаяся возможность восстановления уничтоженной информации не исключает ответственности за уничтожение информации в результате неправомерного доступа к ней.

Под *повреждением компьютерной информации* следует понимать действие виновного лица, в результате которого первоначальное содержание информации хранящейся в компьютере, на ее носителях, в компьютерных системах или их сетях, было утеряно или приобрело искаженную форму.

Под *блокированием компьютерной информации* следует понимать ее закрытие, искусственное затруднение доступа к ней.

Модификация компьютерной информации выражается в изменении ее первоначального состояния (удаление или добавление записей, содержащихся в ее файлах, перевод базы данных на другой язык и т.п.).

Под *копированием компьютерной информации* понимают перенос компьютерной информации на машинный или иной носитель (например, путем записи содержащегося во внутренней памяти ЭВМ файла на дискету, его распечатки и т.п.).

Нарушение работы компьютеров, компьютерных систем или сетей — это временный или устойчивый сбой в работе указанных технических средств, предназначенных для автоматической обработки информации, что не исключает их восстановления (выход из строя программного обеспечения, неверное отображение на мониторе, нарушение порядка выполнения команд и т.п.).

Несанкционированный доступ к охраняемой законом компьютерной

информации, совершенный по неосторожности, исключает правовое основание для привлечения лица к уголовной ответственности.

4. *Субъект* данного преступления — лицо, достигшее 16-ти летнего возраста. Также в качестве субъекта данного преступления законодателем признается и юридическое лицо.

5. *Субъективная сторона* комментируемого преступления характеризуется умышленной виной в виде прямого и косвенного умысла.

В положениях ч. (2) ст. 259 УК РМ предусмотрены обстоятельства, отягчающие ответственность за его совершение, при наличии которых преступление признается более опасным и поэтому влечет более суровое наказание, которые в теории и практике уголовного права признаются *квалифицирующими признаками* преступления. К их числу согласно ч. (2) ст. 259 УК РМ законодатель относит:

b) несанкционированный доступ к компьютерной информации, совершенный двумя или более лицами;

c) несанкционированный доступ к компьютерной информации с нарушением систем защиты;

d) несанкционированный доступ к компьютерной информации, совершенный путем подключения к каналам связи;

e) несанкционированный доступ к компьютерной информации, совершенный с использованием специальных технических средств;

f) с неправомерным использованием компьютера, информационной системы или сети для совершения одного из преступлений, предусмотренных ч. (1), ст.ст. 260^1-260^3, 260^5 и 260^6;

g) в отношении охраняемой законом информации;

h) в особо крупных размерах.

Таким образом, признаки квалифицированного состава рассматриваемого преступления характеризуют либо объективную сторону посягательства, либо субъект преступления.

Статья 260. Неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов

Неправомерные производство, импорт, продажа или иные формы предоставления в пользование технических средств или программных продуктов, разработанных или адаптированных для целей совершения одного из преступлений, предусмотренных статьями 237, 259, 260^1-260^3, 260^5 и 260^6, наказываются штрафом в размере от 500 до 1000 условных единиц или лишением свободы на срок от 2 до 5 лет, а в случае юридического лица —

штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия.

[Ст. 260 в редакции Закона №278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]
[Ст. 260 изменена Законом № 184-XVI от 29.06.2006 г., в силу с 11.08.2006 г.]
[Ст. 260 дополнена Законом № 211-XV от 29.05.2003 г., в силу с 12.06.2003 г.]

1. *Непосредственным объектом* рассматриваемого преступления являются общественные отношения по безопасному производству, импорту, продаже или предоставлению технических средств или программных продуктов, которые могут быть применены в нормальном и законном порядке для сообщения, передачи информационных данных.

Из диспозиции указанной нормы уголовного права исходит, что преступные действия связанные с неправомерным производством, импортом, продажей или предоставлением технических средств или программных продуктов должны быть осуществлены с целью совершения других составов преступления предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ, что придает исследуемой норме уголовного права бланкетный характер. Исходя из требований диспозиций нормы уголовного права — ст. 260 УК РМ, действия виновного лица должны осуществляться, осознано, заведомо с целью совершения других составов преступления, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 и, как следствие этих преступных действий, ими должен быть причинен моральный и материальный ущерб.

Данная норма имеет и факультативный объект посягательства.

Под *факультативным объектом* посягательства выступают личные права граждан, право на свободу и личную неприкосновенность, право на частную собственность, общественная, финансовая, экономическая, информационная и государственная безопасность.

Предмет рассматриваемого преступления — технические информационные средства, или программные продукты которые специально разработаны или адаптированы в целях совершения одного из преступлений предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ.

2. *Объективная сторона* данного преступления характеризуется неправомерным производством, импортом, продажей или предоставлением специальных технических средств или программных продуктов, разработанных и адаптированных с целью совершения хотя бы одного из преступлений, указанных в ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ.

Объективная сторона анализируемого состава преступления предусматривает ее совершение, если было выполнено хотя бы одного из следующих действий:

- неправомерное производство специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерный импорт на территории государства специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерная продажа на таможенной территории Республики Молдова специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерное производство программных продуктов разработанных в целях совершения хотя бы одного из преступлений предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерный импорт программных продуктов, специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерная продажа программного продукта, специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерное предоставление в пользование специальных технических средств, разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ;

- неправомерное предоставление в пользование программных продуктов специально разработанных или адаптированных для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ.

Под *неправомерным производством* специальных технических средств или программных продуктов следует подразумевать противозаконную разработку на научно-технической основе различных электротехнических деталей, их соединение между собой по специальной технологической схеме, доведение их до технического средства как такового, либо программного продукта, разработанного и адаптированного для изготовления банковских расчетных карточек, платежных карточек, либо закрепления текстовой, либо цифровой информации на специальном системном носителе информации, на машинном носителе информации с целью противоправного извлечения из информационных систем, банка данных, необходимую правонарушителю информацию. Из указанной диспозиции нормы уголовного права неправомерное производство специальных технических продуктов, разработанных или адаптированных для совершения других преступлений, может иметь место как на территории Республики Молдова, так и за ее пределами.

Под *неправомерным импортом* специальных технических средств или программных продуктов разработанных или адаптированных с целью совершения других преступлений следует подразумевать их перемещение через таможенную границу государства с полной оплатой таможенной пошлины и таможенных платежей, причитающиеся в соответствие с действующим

таможенным и налоговым законодательством, но с недостоверной заявленной целью их ввоза и применения на территории Республики Молдова.

Под *неправомерной продажей* специальных технических средств или программных продуктов, разработанных и адаптированных для целей совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^{1}-260^{3}, 260^{5} и 260^{6} УК РМ следует подразумевать передачу за наличные деньги либо перечислением технических средств, или программных продуктов собственником, владельцем, производителем, представителем производителя специальных технических средств, или программного продукта получателю (пользователю). Под продажей специальных технических средств или программных продуктов, в исследуемом составе преступления следует так же понимать обмен, дарение, предоставление во временное пользование, а также на бартерной основе на другие товары. Главным определяющим признаком в данном случае должен быть умысел, когда и тот кто отчуждает и тот кто получает специально-техническое средство, или программный продукт разработанный или адаптированный для совершения неправомерных действий, попадающих под признаки одного из составов преступлений, предусмотренных ст.ст. 237, 259, 260^{1}-260^{3}, 260^{5} и 260^{6} УК РМ, а знает о способностях этих средств или продуктов и желает совершить эти действия.

Под *неправомерным предоставлением технических средств или программных продуктов* разработанных или адаптированных действий, попадающих под признаки одного из преступлений предусмотренных ст.ст. 237, 259, 260^{1}-260^{3}, 260^{5} и 260^{6} УК РМ, следует подразумевать сам факт передачи специально изготовленных технических средств или программных продуктов разработанных и адаптированных для совершения противоправных действий, от одного лица другому лицу с целью совершения противоправных действий, попадающих под признаки одного из преступлений, предусмотренных ст.ст. 237, 259, 260^{1}-260^{3}, 260^{5}, и 260^{6} УК РМ.

Неправомерное производство, импорт, продажа или иные формы предоставления специально-технических средств или программных продуктов, их целенаправленная разработка и адаптирование к специальным требованиям, должны быть изготовлены и приспособлены именно для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^{1}-260^{3}, 260^{5} и 260^{6} УК РМ и предполагает совершение в целях их осуществления только активных действий. Вредные последствия по исследуемому составу преступления — ст. 260 УК РМ, наступают, когда совершается одно из преступлений указанных законодателем — 237, 259, 260^{1}-260^{3}, 260^{5} и 260^{6} УК РМ.

Сам вред может быть причинен в виде поделки и ввода в обращения банковских карточек, подложных банковских документов, незаконного доступа к компьютеризированной информации неправомерного перехвата или передачи информационных данных, нарушения целостности информационной системы, воздействия на функционирование информационной системы,

подлог информационных данных, так же как и незаконного извлечения информации, методом информационного мошенничества.

3. *Субъект* рассматриваемого преступления — любое физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-ти летнего возраста. Если неправомерное производство, импорт, продажу или предоставление технических средств или программных продуктов совершил представитель юридического лица, то, в соответствии с ч. (3) ст. 21 УК РМ, к уголовной ответственности будет привлекаться юридическое лицо, которое осуществило неправомерное производство, импорт, продажу или предоставление технических средств или программных продуктов, разработанных и адаптированных для совершения преступлений предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ.

4. *Субъективная сторона* этого преступления характеризуется прямым умыслом. Законодатель в ст. 260 УК РМ указывает на заведомый характер деятельности виновного. Осуществляя неправомерное производство, импорт, продажу или иные формы предоставления специально изготовленных технических средств или программных продуктов, их целенаправленную разработку и адаптирование к специальным требованиям должны быть, изготовлены и приспособлены именно для совершения одного из преступлений, предусмотренных ст.ст. 237, 259, 260^1-260^3, 260^5 и 260^6 УК РМ. Виновный сознает характер своих действий, предвидит возможность поделки и ввода в обращение банковских карточек, подложных банковских документов, незаконного доступа к компьютеризированной информации, неправомерного перехвата, передачи информационных данных, уничтожения, модификации, блокирования, извлечения информационных данных путем мошенничества и желает совершить эти действия.

Цель и мотивы преступления не являются обязательными признаками субъективной стороны и на квалификацию содеянного не влияют.

Статья 260^1. Неправомерный перехват передачи информационных данных

Неправомерный перехват передачи информационных данных (включая электронную эмиссию), не предназначенных для общего пользования, передаваемых в информационную систему, исходящих из нее или осуществляемых внутри такой системы, наказывается штрафом в размере от 500 до 1000 условных единиц или лишением свободы на срок от 2 до 5 лет, а в случае юридического лица — штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия.

[Ст. 260^1 введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. *Непосредственным объектом* рассматриваемого состава преступления являются общественные отношения обеспечивающие *конфиденциальность передаваемой информации* по компьютерным, информационным сетям и системам, включая и электронную эмиссию информации, которая не предназначена для общего пользования. Сама передача конфиденциальных данных, не предназначенных для общего пользования по компьютерным информационным сетям и системам, в том числе электронную эмиссию информации конфиденциального характера является своего рода правом человека, которое гарантировано ст. 30 Конституцией РМ. Право человека находящегося на территории государства, независимо от его гражданства, касающееся передачи информации, корреспонденции не предназначенных для общего пользования охраняется также ст. 8 Международной Конвенции по правам человека от 4 ноября 1950 г.

В качестве *факультативного объекта* данного состава преступления следует признать права граждан на защиту конфиденциальных данных, не предназначенных для общего пользования, представляющие данные о личной жизни, корреспонденции, научные сведения, сведения об интеллектуальной собственности, произведения искусства, сведения об экономической, общественной, энергетической безопасности, и т.д.

Предмет рассматриваемого преступления — информационные данные (включая электронную эмиссию данных) конфиденциального характера, не предназначенные для общего пользования.

2. *Объективная сторона* данного преступления характеризуется исполнением хотя бы одного из следующих неправомерных действий направленных на:

- перехват посредством любых механизмов и технических средств, информационных данных передаваемых в информационных сетях;
- перехват посредством любых средств и методов передаваемой информации, конфиденциального характера, по специальным кабельным каналам телефонной связи;
- перехват посредством специальных технических средств, передаваемой информации, предназначенной для сообщения по каналам искусственных спутников Земли;
- проникновения в информационную сеть Интернет с целью перехвата передаваемой информации между ее абонентами.

Под *перехватом* информации, информационных данных следует понимать любые действия направленные на неправомерное прослушивание, регистрацию, фиксирование, улавливание, либо проверки лицом которое не имеет на это какие либо основания телефонного разговора, или обыкновенной корреспонденции между двумя лицами.

Под *передачей* информационных данных следует подразумевать отправление от отправителя текстуальных или цифровых данных к получателю, по каналам телефонной, телеграфной, факсимильной и кабельной электрической

связи. Информационные данные могут быть переданы от отправителя к получателю и посредством электромагнитных волн, электроносителей, электроимпульсов по установленной сети Интернет между абонентами, независимо от их месторасположения и местонахождения.

Преступление предусмотренное ст. 260^1 УК РМ следует считать оконченным с момента неправомерного и несанкционированного подключения к линиям, каналам, средствам по которым осуществляется передача информационных данных с целью прослушивания, перехвата, фиксирования передаваемой информации, не предназначенной для общего пользования.

3. *Субъект* рассматриваемого преступления — любое физическое вменяемое лицо достигшее на момент совершения преступления 16-ти летнего возраста. В случаях если неправомерный перехват передачи информационных данных будет осуществляться юридическим лицом, то в таких случаях в соответствии с ч. (3) и ч. (4) ст. 21 УК РМ к уголовной ответственности, будет привлекаться юридическое лицо, которое осуществило или попыталось осуществить неправомерный перехват передачи информационных данных по существующим каналам, сетям между абонентами либо отправителем и получателем.

4. *Субъективная сторона* рассматриваемого преступления характеризуется исключительно прямым умыслом. Подключившись незаконным способом к линиям, каналам через которые осуществляется передача информационных данных и сообщений при помощи технических средств посредством которых виновный прослушивает, записывает, фиксирует передаваемую информацию, он осознает неправомерный характер своих действий, предвидит возможность получения необходимых ему данных, не предназначенных для общего пользования и желает совершить противоправные действия.

Цель и мотивы исследуемого преступления не являются обязательными признаками субъективной стороны и на квалификацию содеянного не влияют.

Статья 260^2. Нарушение целостности информационных данных, содержащихся в информационной системе

Преднамеренное изменение, удаление или повреждение информационных данных, содержащихся в информационной системе, либо неправомерное ограничение доступа к этим данным, несанкционированное перемещение информационных данных из информационной системы, базы данных, приобретение, продажа или иные формы предоставления в пользование информационных данных ограниченного доступа, если эти действия повлекли причинение ущерба в крупных размерах, наказываются штрафом в размере от 500 до 1000 условных единиц или лишением свободы на срок от 2 до 5 лет.

[Ст. 260^2 введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. *Непосредственным объектом* преступления предусмотренного ст. 260^2 УК РМ являются общественные отношения, обеспечивающие целостность, точность, достоверность и сохранность информационных данных содержащихся в информационной системе на электронных носителях, на которые и направлены преступные посягательства.

Разработчиками информационных данных, их авторами, абонентами подключенными на законных основаниях к линиями, средствам и каналам для осуществления точности, целостности и своевременности передачи данных, как общего, так и конфиденциального содержания обеспечивается со стороны законных владельцев линии, сети, канала право на полную, точную, своевременную и качественную информацию. Поэтому в случаях преступного посягательства на целостность информационных данных с целью их изменения, удаления, повреждения или искажения одновременно осуществляется посягательство на права граждан, юридических лиц на сохранение, целостности, точности и конфиденциальности информации принадлежащий им и находящейся под определенной государственной гарантией, предусмотренной нормами гражданского и уголовного права в информационной системе, сетях, каналах на электронных носителях информации.

Предмет рассматриваемого преступления — информационные данные, содержащиеся в информационной системе, сетях, каналах специальных технических средствах, электромагнитных технических средствах, информационные данные, находящиеся на электронных носителях посредством, которых передаются информационные данные законным пользователям и получателям.

2. *Объективная сторона* комментируемого преступления характеризуется неправомерными действиями направленными на нарушение целостности информационных данных, представленных законными владельцами, разработчиками, собственниками, содержащихся в информационной системе качество, количество, полнота и конфиденциальность которой гарантировано законному пользователю информационной системы, сети, канала, других технических средств.

Объективная сторона анализируемого состава преступления предусматривает одно из следующих действий:

- изменение целостности, либо содержания, информационных данных содержащихся в информационной системе, информационной сети, информационном канале, в базе данных, на информационном электроном носителе, предназначенном для эмиссии информации;

- удаление информационных данных, находящиеся и содержащихся в информационной системе, в информационной сети, в базе данных, на электронных носителях информации;

- повреждение информационных данных, находящихся и содержащихся в информационной системе, в информационной сети, в базе данных, на электронных носителях информации;

- неправомерное ограничение доступа к информационным данным находящимся и содержащимся в информационной системе, информационной сети, в базе данных, на электронных носителях;

- несанкционированное перемещение информационных данных из информационной системы, из информационной сети, из электронных носителей информации;

- несанкционированное перемещение информационных данных из баз данных информационной системы, информационной сети, из базы данных электронных носителей информации;

- несанкционированное приобретение информационных данных ограниченного доступа из информационной системы;

- несанкционированную продажу информационных данных ограниченного доступа из информационной системы;

- совершение иных несанкционированных действий предоставления в пользование информационных данных ограниченного действия, повлекшие за собой ограничение доступа к информационным данным, несанкционированное перемещение информационных данных из базы данных, их приобретения и продажу, а также их уничтожение или исчезновение.

Одним из обязательных признаков объективной стороны исследуемого состава преступления является причинение ущерба в крупных размерах. Вместе с тем законодатель четко и определенно не указывает, кому непосредственно должен быть причинен ущерб. Мы полагаем, что ущерб в подобных случаях может быть нанесен владельцам, собственникам информации содержащейся в информационных сетях, базам данных на электронных носителях информации, а также владельцам информационной системы, информационных носителей, электронных носителей информации, собственникам любых технических средств, подключенных и находящихся на законном основании в информационной системе, информационной сети, предназначенных для сохранения, передачи, либо приема информационных данных. В соответствии со ст. 126 УК РМ ущербом в крупных размерах признается ущерб, превышающий 2500 условных единиц (более 50000 молдавских лей).

Под *изменением* информационных данных следует понимать замену, перевод, изменение данных текстуального, цифрового, звукового характера осуществляемых в результате неправомерного проникновения в информационные данные ограниченного доступа.

Под *удалением информационных данных* следует понимать противоправное действие виновного лица с целью уничтожения, ликвидации информации накопившейся и находящейся на технических средствах носителей информации.

Под *повреждением информационных данных* следует понимать противоправные умышленные целенаправленные действия, совершаемые с целью уничтожения, порчи, повреждения, информации с целью ее извлечения и

удаления из информационной системы, информационной сети, из базы данных, либо из блока памяти специальных технических средств, где находились и хранились информационные данные.

3. *Субъекты* рассматриваемого преступления — любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-ти летнего возраста. В случае если противоправные действия по факту нарушения целостности информационных данных содержащихся в информационной системе с целью изменения, удаления или повреждения информационных данных, либо несанкционированное перемещение информационных данных из информационной системы базы данных были совершены юридическим лицом, то в соответствии с ч. (3) и ч. (4) ст. 21 УК РМ субъектом преступления будет признаваться юридическое лицо, которое посягало на нарушение целостности информационных данных, содержащихся в информационной системе.

4. *Субъективная сторона* рассматриваемого преступления характеризуется только прямым умыслом. Законодатель четко и определенно в диспозиции ст. 260^2 УК РМ указывает на заведомый противоправный характер совершенных преступных действий.

Поскольку исследуемый состав преступления имеет как формальный, так и материальный характер, цель и мотивы совершения данного преступления четко определенны законодателем в норме права, являются обязательными признаками субъективной стороны и прямо влияют на правовую квалификацию содеянного преступления.

Статья 260^3. Воздействие на функционирование информационной системы

(1) Воздействие на функционирование информационной системы путем ввода, передачи, изменения, удаления или повреждения информационных данных или ограничения доступа к этим данным, если эти действия повлекли причинение ущерба в крупных размерах, наказывается штрафом в размере от 700 до 1000 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 150 до 200 часов, или лишением свободы на срок от 2 до 5 лет, а в случае юридического лица — штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия.

(2) То же действие:

a) совершенное в корыстных целях;

b) совершенное двумя или более лицами;

c) совершенное организованной преступной группой или преступной организацией;

d) повлекшее причинение ущерба в особо крупных размерах, наказывается штрафом в размере от 700 до 1000 условных единиц или лишением свободы на срок от 3 до 7 лет, а в случае юридического лица — штрафом в размере от 3000 до 6000 условных единиц или ликвидацией предприятия.

[Ст. 260[3] введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. *Непосредственным объектом* рассматриваемого состава преступления являются общественные отношения регулирующие нормальное и безопасное функционирование информационной системы.

Из диспозиции комментируемой нормы исходит что преступные действия связанные с воздействием на функционирование информационной системы должны быть осуществлены путем ввода передачи, изменения, удаления или повреждения информационных данных или ограничения доступа к этим данным, и как следствие этих преступных действий должен быть причинен моральный, либо материальный ущерб законному владельцу информационной системы.

Факультативным объектом выступают личные права граждан на свободное сообщение информационных данных, конфиденциальность и неприкосновенность передаваемой информации по информационной системе, информационным каналам через специальные электронные носители информации.

Предмет рассматриваемого преступления — информационная система, специальные электронные носители информации в которых находится накопившаяся информация, предназначенная для сообщения, передачи пользователям, получателям.

2. *Объективная сторона* данного преступления характеризуется непосредственным воздействием на нормальное функционирование информационной системы с целью искажения, изменения, удаления данных находившихся на законном основании в информационной системе, предназначенных для сообщения, передачи по каналам информационной системы.

Объективная сторона анализируемого состава преступления предусматривает совершение, альтернативно, одного из следующих действий:

- неправомерный ввод данных в информационную систему, в которой находятся накопившиеся данные, предназначенные для отправления, сообщения по информационным каналам, системы, через электромагнитные носители информации получателям, потребителям;
- неправомерное воздействие на функционирование информационной системы путем передачи информационных данных по информационной системе;
- изменение информационных данных, находящихся в информационной системе;
- удаление информационных данных, находящихся в информационной системе;

- повреждение информационных данных, находящихся в информационной системе;

- неправомерное ограничение доступа к информационным данным, находящимся в информационной системе.

В диспозиции исследуемой нормы законодатель четко указывает, что вышеуказанные противоправные действия будут признаны и квалифицированы как преступление только в случае если в результате их совершения владельцу информационной системы будет причинен ущерб в крупном размере.

Под *воздействием* на функционирование действующей информационной системы следует понимать не что иное, как влияние на нормальную работу и функционирование информационной системы.

Под *вводом* информации в функционирование информационной системы следует понимать любые добавления к данным находящиеся уже в информационной системе.

Под *передачей* информационных данных следует понимать неправомерное и несанкционированное сообщение информации ограниченного доступа широкой публике посредством технических средств сообщения, через электромагнитные носители информации.

Под *изменением* информационных данных следует понимать неправомерное проникновение в информационную систему, к информации ограниченного характера, и осознанного осуществления изменений в существующей информации в информационной системе, базе данных.

Под *удалением* информационных данных следует понимать противоправное несанкционированное действие виновного лица совершаемого с целью уничтожения, ликвидации, исключения имеющейся информации закрепленной в техническом средстве, электромагнитном средстве, информационной системе, а также ее исключения из информационной системы из информационного канала целиком или частично.

Под *повреждением* информационных данных следует понимать целенаправленные умышленные действия, совершаемые виновным лицом которые направлены на порчу информационной программы, информационной системы, либо базы данных в которой содержится накопившаяся информация, либо электромагнитные носители информации.

Под *ограничением доступа* к информационным данным следует понимать противоправные действия, совершаемые виновным лицом с целью ограничения, ограждения, воспрепятствования проникновения в информационную систему, на электромагнитном носителе информации, в информационную программу.

3. Согласно ч. (2) ст. 260^3 УК РМ, законодатель предусматривает следующие отягчающие обстоятельства, при воздействии на функционирование информационной системы путем ввода, передачи, изменения, удаления или повреждения информационных данных или ограничения доступа к этим данным:

a) совершенное в корыстных целях;

b) совершенное двумя или более лицами;

c) совершенное организованной преступной группой или преступной организацией;

d) повлекшее причинение ущерба в особо крупных размерах.

4. *Субъект* рассматриваемого преступления — любое физическое вменяемое лицо, достигшее к моменту совершения преступления, 16-ти летного возраста, а так же юридическое лицо.

5. *Субъективная сторона* комментируемого преступления характеризуется прямым умыслом. Законодатель четко и определенно указывает на заведомо противоправный характер деятельности виновного лица. Воздействуя на нормальное функционирование информационной системы путем незаконного и несанкционированного ввода, передачи, изменения, удаления или повреждения информационных данных или ограничения доступа к данным хранящимся в информационной системе, на базе данных, виновное лицо сознает характер своих неправомерных действий, предвидит возможность отрицательного воздействия на нормальное функционирование информационной системы и желает совершать преступные действия.

Цель и мотив совершения данного преступления не являются обязательными признаками субъективной стороны и на правовую квалификацию содеянного не влияют.

В соответствии с ч. (2) ст. 260^3 УК РМ, законодатель предусмотрел следующие квалифицированные признаки:

a) совершенное в корыстных целях;

b) совершенное двумя или более лицами;

c) совершенное организованной преступной группой или преступной организацией;

d) повлекшее причинение ущерба в особо крупных размерах.

Законодатель предусматривает неосторожную форму вины по отношению к наступившим тяжким последствиям. Виновный предвидит абстрактную возможность наступления тяжких последствий, как результат своих противоправных действий, описанных в ч. (1) ст. 260^3 УК РМ, но самонадеянно рассчитывает их предотвратить; не предвидит возможности наступления тяжких последствий, хотя должен и мог предвидеть их наступление.

Статья 260^4. Неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных

(1) Неправомерные производство, импорт, продажа или иные формы предоставления в пользование пароля, кода доступа или иных аналогичных данных, с помощью которых может быть получен

доступ к информационной системе в целом или ее части с целью совершения одного из преступлений, предусмотренных статьями 237, 259, 2601-2603, 2605 и 2606, если эти действия повлекли причинение ущерба в крупных размерах, наказываются штрафом в размере от 500 до 1000 условных единиц или лишением свободы на срок от 2 до 5 лет, а в случае юридического лица — штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

(2) Те же действия:

a) совершенные в корыстных целях;

b) совершенные двумя или более лицами;

c) совершенные организованной преступной группой или преступной организацией;

d) повлекшие причинение ущерба в особо крупных размерах, наказываются штрафом в размере от 1000 до 1500 условных единиц или лишением свободы на срок от 3 до 7 лет, а в случае юридического лица — штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия.

[Ст. 260[4] введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. *Непосредственным объектом* рассматриваемого преступления являются общественные отношения, обеспечивающие нормальное производство, импорт, продажу или предоставление паролей, кодов доступа или иных аналогичных данных применяемых для доступа к информационной системе, базе данных к электромагнитным носителям для передачи или получения информации.

Факультативным объектом являются личные права граждан на ведение свободной корреспонденции по каналам информационной сети, информационной системы, а также права на свободу и неприкосновенность осуществляемой корреспонденции посредством электронных носителей информационной системы, право на частную собственность и ее охрану, экономическая, общественная и государственная безопасность Республики Молдова в целом.

Предметом рассматриваемого преступления выступают пароли, коды или иные аналогичные данные посредством которых осуществляется доступ к информационной системе, а так же сама информация в целом или определенной ее части находящаяся в информационной системе, базе данных на электромагнитных носителях информационной системы, в том числе и в компьютерных программах.

2. *Объективная сторона* преступления предусмотренного ст. 260[4] УК РМ характеризуется неправомерными действиями направленными

на производство, импорт, продажу или предоставление паролей, кодов, обеспечивающих доступ к информации находящийся и хранившийся в информационной системе.

Объективная сторона анализируемого состава преступления предусматривает его совершение, если виновным лицом было выполнено хотя бы одно из следующих действий:

- неправомерное производство пароля, кода, обеспечивающее доступ к информационной системе;
- неправомерный импорт на территории государства паролей, кодов обеспечивающих доступ к информационной системе;
- неправомерную продажу паролей, кодов обеспечивающих доступ к информационной системе;
- неправомерное представление других аналогичных данных, кроме паролей, кодов, обеспечивающих доступ к информационной системе.

Под *неправомерным производством* паролей, кодов следует понимать совершение противоправных действий направленных на изготовление, создание паролей, кодов, которые в случае несанкционированного подключения к информационной системе могут навредить, разрушить информацию, находящуюся в информационной системе.

Под *импортом* паролей, кодов, обеспечивающих доступ к информационной системе следует понимать ввоз на территорию государства информационных технических средств изготовленных за пределами Республики Молдова, в которых установлены специальные информационные данные которые могут образовать пароли и коды необходимые для подключения к информационной системе.

Под *продажей* паролей, кодов, обеспечивающих подключение к информационной системе, следует понимать неправомерное изготовление с последующим отчуждением специальных технических машин, технических средств, программ, которые могут быть снабжены техникой обеспечивающей составление паролей, кодов необходимых для неправомерного подключения к информационной системе.

Под *паролем* следует понимать секретное условное слово, в случае применения которого только лица знающие пароль могут проверять деятельность других лиц, подключенных к информационной системе. В случае неправомерного предоставления пароли (условного слова) другим лицам, если ими были совершены несанкционированное подключения к информационной сети либо к информационной системе с целью извлечения из нее информационных данных, то на лицо будет состав преступления, предусмотренный ст. 260^4 УК РМ.

Под *кодом подключения* к информационной системе следует понимать набор цифр, знаков, условных обозначений которые могут послужить для передачи каких-либо сообщений или информации.

Под *иными аналогичными данными, с помощью которых может быть получен доступ к информационной системе в целом или к ее части* следует понимать набор информации, переданной, посланной правонарушителем другому лицу, которое в сопоставлении с другими данными, методом исключения, применяет ее для исчисления ключа обеспечивающего доступ к информационной сети, информационному каналу, к электромагнитному носителю информации.

Под *доступом к информационной системе в целом или к ее части* следует понимать совершение противоправных действий с целью проникновения или прорыва информационной сети, базы данных, электромагнитных носителей информации, либо информационных систем и уровень совершения доступа, по частям или в целом.

В соответствии с ч. (2) ст. 260^4 УК РМ, в качестве квалифицированных признаков исследуемого состава преступления признаются:

a) совершенные в корыстных целях;

b) совершенные двумя или более лицами;

c) совершенные организованной преступной группой или преступной организацией;

d) повлекшие причинение ущерба в особо крупных размерах.

Преступление считается оконченным, если в результате совершения противоправных действий был причинен ущерб в крупных, либо особо крупных размерах.

3. *Субъект* рассматриваемого преступления — физическое вменяемое лицо, достигшее к моменту совершения преступления, 16-ти летного возраста либо юридическое лицо.

4. *Субъективная сторона* комментируемого преступления характеризуется прямым умыслом, виновного лица. Виновные лицо сознает характер своих неправомерных действий, предвидит возможность производства, импорт, продажу или предоставления иными незаконными действиями, кодов, паролей, посредством которых противоправным способом осуществляется несанкционированное подключение к информационной системе и желает совершить эти противоправные действия.

Статья 260^5. Подлог информационных данных

Неправомерные ввод, изменение или удаление информационных данных либо ограничение доступа к этим данным, влекущие выдачу недостоверных данных с целью использования их для производства определенных юридических последствий, наказываются штрафом в размере от 1000 до 1500 условных единиц или лишением свободы на срок от 2 до 5 лет.

[Ст. 260^5 введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. Под *подлогом информационных данных* следует понимать неправомерное умышленное действие, осуществляемое путем ввода, порчи, устранения, либо сокрытия компьютерной информации с целью получения недостоверных данных, необходимых виновному лицу для использования в производстве юридических последствий.

2. *Непосредственным объектом* исследуемого состава преступления являются общественные отношения, обеспечивающие нормальную работу информационной системы, безопасность информационных систем, электромагнитных носителей информации, а также правовые отношения, на которых основывается в процессе своей нормальной работе информационный сети, информационные системы, электромагнитные машины носителей и хранителей информационных данных.

Под *факультативным объектом* данного преступления следует признать права граждан на личную свободу, на осуществление корреспонденции по информационной сети, системы, в также на личную неприкосновенность информации находящейся в информационной системе, а также право на осуществление конфиденциальной переписки и сообщения информационных данных по информационной системе, электромагнитных носителей информации со своими абонентами информационной сети.

Предмет рассматриваемого преступления обрабатываемая хранящаяся, информация в компьютерных системах данных, подтверждающаяся при наличии определенных программ, документов, кодов, баз данных.

Объективная сторона данного состава преступления предусматривает ее совершение, если было выполнено хотя бы одно из следующих неправомерных действий:

- ввод информационных данных, влекущих выдачу недостоверных данных с целью использования их для производства определенных юридических действий;
- изменение информационных данных, влекущих выдачу недостоверных данных с целью использования их для производства определенных юридических последствий;
- удаление информационных данных, влекущих выдачу недостоверных данных с целью использования их для производства определенных юридических действий;
- ограничение доступа к информационным данным, влекущих выдачу недостоверных данных с целью использования их для производства и осуществления определенных юридических действий.

4. *Субъект* рассматриваемого преступления — физическое, вменяемое лицо, достигшее к моменту совершения преступления, 16-ти летного возраста. К уголовной ответственности в качестве субъекта преступления предусмотренного ст. 260^5 УК РМ может привлекаться юридическое лицо.

5. *Субъективная сторона* исследуемого состава преступления характеризуется прямым умыслом.

Статья 260⁶. Информационное мошенничество

(1) Ввод, изменение или удаление информационных данных, ограничение доступа к этим данным или иные способы препятствования функционированию информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли причинение ущерба в крупных размерах, наказываются штрафом в размере от 1000 до 1500 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 150 до 200 часов, или лишением свободы на срок от 2 до 5 лет.

(2) Те же действия:

a) совершенные организованной преступной группой или преступной организацией;

b) повлекшие причинение ущерба в особо крупных размерах, наказываются лишением свободы на срок от 4 до 9 лет.

[Ст. 260⁶ введена Законом № 278-XVI от 18.12.2008 г., в силу с 20.02.2009 г.]

1. Под *информационным мошенничеством* следует понимать противоправное умышленное несанкционированное действие, в результате которого был нанесен ущерб интеллектуальной собственности другого лица посредством следующих средств и обстоятельств:

- любой ввод, нарушение, отключение, удаление, либо сокрытие компьютеризированной информации;

- любое подключение к функционирующей компьютеризированной информационной системе, совершаемое с обманным умыслом или незаконной экономической выгодой для себя или для другого лица.

2. *Непосредственным объектом* рассматриваемого преступления являются общественные отношения обеспечивающие целостность и безопасность информационной системы, информационной сети, электромагнитных носителей информации, других составляющих машин, инструментов, обеспечивающих нормальную и правомерную работу информационной системы, информационной сети.

В диспозиции данной нормы предусмотрено, что преступные действия связанные с вводом, изменением, удалением информационных данных, либо ограничением доступа к этим информационным данным, или иные способы препятствования функционированию информационной системы должны осуществляться *с целью извлечения материальной выгоды* для виновного или иного лица и при условии, что в результате совершения противоправных действий законному владельцу информационной системы был причинен *ущерб в крупных размерах.*

Под *факультативным объектом* выступают личные права граждан — абонентов информационной сети, информационной системы на обеспечение

хранения информационных данных в информационной сети, информационной системы, на конфиденциальность ведения переписки, сообщения с абонентами по информационной сети, информационной системы, электромагнитных носителей информации.

Предмет рассматриваемого преступления — полученная, обрабатываемая и хранящаяся информация в компьютерной информационной системе, информационной сети, на электромагнитных носителях информации, базе данных информационной системы, а также в базе данных других технических средств информационной системы или сети, которые в силу своих технических параметров могут на законном основании выдавать сведения об имеющихся информационных данных находящихся в информационной сети, передачи, отправления информации к абонентам, либо пользователям информационной сети или информационной системы.

3. *Объективная сторона* исследуемого состава преступления предусматривает ее совершение, если было выполнены хотя бы одно из следующих неправомерных умышленных действий:

- ввод информационных данных в функционирование информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли за собой причинения ущерба в крупных размерах;
- изменение информационных данных в функционировании информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли за собой причинение ущерба в крупных размерах;
- удаление информационных данных из существующей и функционирующей информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли за собой причинение ущерба в крупных размерах;
- ограничение доступа к информационным данным в функционирующей информационной системе с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли за собой причинение ущерба в крупных размерах;
- совершение иным способом препятствования нормальному и законному функционированию информационной системы с целью извлечения материальной выгоды для себя или иного лица, если эти действия повлекли за собой причинение ущерба в крупных размерах.

Ввод, изменение, удаление информационных данных, ограничение доступа к информационным данным находящимся в функционирующей и действующей информационной системе, а также совершение иных способов препятствующих нормальному функционированию информационной системы предполагает только активные действия.

Под *воспрепятствованием* нормальному функционированию существующей информационной системы подразумеваем, совершение конкретных

противоправных действий направленных на остановку, блокирование, создание препятствий, которые повлияли бы на функционирование самой информационной системы, в отношении которого направлены противоправные действия виновного лица.

Под *извлечением материальной выгоды* следует понимать получение определенной выгоды, выраженной в деньгах либо в реальных предметах и ценностях.

Объективная сторона комментируемого преступления предусматривает следующие квалифицирующие признаки:

a) совершение информационного мошенничества организованной группой или преступной организацией;

b) совершение информационного мошенничества повлекшее причинение ущерба в особо крупных размерах.

4. *Субъект* рассматриваемого преступления — любое физическое вменяемое, лицо достигшее к моменту совершения преступления, 16-ти летного возраста. В случае если информационное мошенничество, было совершено юридическим лицом, то к уголовной ответственности в соответствии с ч. (3) и ч. (4) ст. 21 УК РМ будет привлекаться виновное юридическое лицо.

5. *Субъективная сторона* исследуемого состава преступления характеризуется наличием прямого умысла виновного лица. Осуществив неправомерный ввод, изменение или удаление информационных данных, либо ограничение доступа к информационным данным находящимся в существующей и действующей информационной системе, или иные способы препятствующие функционированию информационной системы с целью извлечения материальной выгоды для себя или иного лица виновное лицо сознает противоправный характер своих преступных действий, предвидит возможность противоправного ввода, изменения или удаления информационных данных, как и других противоправных действий по поводу ограничения доступа к информационным данным или иных способов препятствовавших функционированию существующей информационной системы, и желает совершить эти противоправные действия.

Статья 261. Нарушение правил безопасности информационных систем

Нарушение правил сбора, обработки, хранения, распространения, распределения информации или правил защиты информационных систем, предусмотренных в соответствии с видом информации или степенью ее защиты, если это действие способствовало хищению, искажению, уничтожению информации или повлекло иные тяжкие последствия, наказывается штрафом в размере

до 400 условных единиц, или неоплачиваемым трудом в пользу общества на срок от 200 до 240 часов, или лишением свободы на срок до 2 лет с лишением или без лишения во всех случаях права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, а юридическое лицо наказывается штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

[Ст. 261 изменена Законом № 211-XV от 29.05.2003 г., в силу с 12.06.2003 г.]

1. *Непосредственным объектом* исследуемого преступления являются общественные отношения, регламентирующие порядок *собирания, обработки, хранения, распространения, и распределения компьютерной информации,* способствующей нормальному режиму работы информационных систем, а также предусмотренные внутренними правоприменительными актами, отношения в области обеспечения технической защиты и безопасности информационных систем.

Техническая защита компьютерной информации в ЭВМ, их системах либо компьютерных сетях обеспечивается комплексом конструкторских, организационных, программных и технических мероприятий на всех этапах их создания и эксплуатации. Основными методами и средствами технической защиты компьютерной информации являются: использование защищенных средств; регламентирование работы пользователей, технического персонала, программных средств, элементов баз данных и носителей информации (разграничение доступа), регламентирование размещения автоматизированных систем и средств вычислительной техники, инженерно-технического оборудования сооружений и коммуникаций, предназначенных для эксплуатации автоматизированных систем и средств вычислительной техники; поиск, выявление и блокирование закладных устройств.

2. *Объективная сторона* данного состава преступления выражается в нарушении правил эксплуатации ЭВМ, их систем либо компьютерных сетей (действие или бездействие), определенных их:

1) владельцем, уполномоченным им лицом или распорядителем таких ЭВМ, их систем либо компьютерных сетей, или

2) производителем ЭВМ, их систем, компьютерных сетей или их программного обеспечения.

Обязательными признаками объективной стороны являются последствия в виде:

- утечки информации вследствие ее хищения или копирования;
- хищения средств защиты компьютерной информации;
- искажения или уничтожения компьютерной информации или средств ее защиты;
- существенного нарушения работы ЭВМ, их систем либо компьютерных

сетей, а также причинная связь между действиями и последствиями. Утечка информации может быть связана также с ее утратой (уничтожением или повреждением).

Последствия в виде искажения или уничтожения компьютерной информации или средств ее защиты и существенного нарушения работы ЭВМ, их систем либо компьютерных сетей могут быть вызваны действиями (бездействием) как лиц, которые осуществляют их эксплуатацию либо отвечают за техническое или иное обеспечение их надлежащей эксплуатации, так и действиями иных, посторонних лиц, а в виде расхищения компьютерной информации, ее незаконного копирования или расхищения средств защиты компьютерной информации — только действиями посторонних лиц, не являющихся ответственными за эксплуатацию ЭВМ, их систем либо компьютерных сетей.

Нарушения правил эксплуатации ЭВМ, их систем либо компьютерных сетей может выражаться в нарушении правил эксплуатации их аппаратного обеспечения или в нарушении правил эксплуатации их программного обеспечения. Нарушением правил эксплуатации ЭВМ может признаваться также невыполнение или ненадлежащее выполнение обязанностей по техническому обеспечению защиты компьютерной информации, в частности, по поиску, выявлению и блокированию закладных устройств.

Нарушение установленных норм и требований технической защиты компьютерной информации подразделяются на три категории: *первая* — невыполнение норм и требований технической защиты компьютерной информации, в результате чего создается реальная возможность нарушения целостности этой информации или ее утечки по техническим каналам; *вторая* — невыполнение норм и требований технической защиты компьютерной информации, в результате чего создаются предпосылки для нарушения целостности этой информации или ее утечки; *третья* — невыполнение иных требований технической защиты информации с ограниченным доступом.

О понятиях *"хищение"*, *"искажение" и "уничтожение"* компьютерной информации смотри соответственно в комментарии к ст. 259 УК РМ. Хищение компьютерной информации может быть совершено путем несанкционированного доступа к ней, приема и анализа побочных электромагнитных излучений и наводок, использования закладных устройств.

Средства защиты компьютерной информации — это технические устройства и (или) технологические разработки, предназначенные для создания технологического препятствия несанкционированному доступу к компьютерной информации.

Копирование компьютерной информации — это ее воспроизведение в электронном виде, перенесение на иной носитель информации с использованием программных и (или) технических средств ЭВМ. Копирование компьютерной информации без использования программно-технических средств ЭВМ,

например, путем сканирования излучения монитора специальными техническими средствами, должно рассматриваться как ее хищение.

Признание нарушения работы ЭВМ, их систем либо компьютерных сетей *существенным* зависит от длительности прерывания их работы, сложности и длительности их ремонта и т.п.

3. С *субъективной стороны* преступление характеризуется косвенным умыслом и неосторожностью в отношении последствий в виде расхищения, искажения или уничтожения компьютерной информации, средств ее защиты, незаконного копирования компьютерной информации или существенного нарушения работы ЭВМ, их систем либо компьютерных сетей. Само же нарушение правил эксплуатации ЭВМ, их систем либо компьютерных сетей может быть как умышленным, так и неосторожным.

4. *Субъект* преступления специальный — физическое, вменяемое лицо, достигшее 16-ти летнего возраста, отвечающее за эксплуатацию ЭВМ, их систем или компьютерных сетей. В соответствии с ч. (3) и ч. (4) ст. 21 УК РМ субъектом преступления, в случае совершения им противоправных действий, предусмотренных ст. 261 УК РМ может быть признано и юридическое лицо.

Статья 261[1]. Несанкционированный доступ к сетям и услугам электросвязи

(1) Несанкционированный доступ к сетям и/или услугам электросвязи с использованием сетей и/или услуг электросвязи других операторов, повлекший причинение ущерба в крупных размерах, наказывается штрафом в размере от 500 до 1000 условных единиц или лишением свободы на срок до 1-го года, а юридическое лицо наказывается штрафом в размере от 1000 до 3000 условных единиц с лишением права заниматься определенной деятельностью.

(2) То же действие:

[Пкт. a) исключен Законом № 277-XVI от 18.12.2008 г., в силу с 24.05.2009 г.]

b) совершенное двумя или более лицами;

c) совершенное с нарушением систем защиты;

d) совершенное с использованием специальных технических средств;

e) повлекшее причинение ущерба в особо крупных размерах, наказывается штрафом в размере от 1000 до 3000 условных единиц или лишением свободы на срок до 5 лет, а юридическое лицо наказывается штрафом в размере от 3000 до 6000 условных единиц с лишением права заниматься определенной деятельностью.

[Ст. 261[1] изменена Законом № 277-XVI от 18.12.2008 г., в силу с 24.05.2009 г.]
[Ст. 261[1] изменена Законом № 184-XVI от 29.06.2006 г., в силу с 11.08.2006 г.]
[Ст. 261[1] введена Законом № 254-XV от 09.07.2004 г., в силу с 22.10.2004 г.]

1. *Непосредственным объектом* состава преступления предусмотренного ст. 161[1] УК РМ являются общественные отношения в сфере охраны сетей телефонной связи и телефонных аппаратов, а также общественные отношения в сфере охраны оказания услуг со стороны телефонных операторов при осуществлении ими заказных телефонных переговоров между телефонными абонентами.

В качестве *предмета* данного преступления выступают телефонные линии электрической связи, протянутые от центральной телефонной станции до телефонных абонентов, линии телефонной связи, протянутые между телефонными абонентами, расположенные на территории Республики Молдова.

В качестве *основного предмета* преступления следует признать и телефонные аппараты, которые присоединены в конце линии электрической связи, посредством которых осуществляются телефонные переговоры между абонентами. В качестве *факультативного предмета* совершения данного преступления следует признать устную информацию, которая сообщается между телефонными абонентами, ведущими переговоры между собой посредством телефонных аппаратов, присоединенных между собой специальной телефонной линией связи. Также в качестве факультативного предмета данного преступления необходимо признать и письменную, от руки или печатаную информацию, которая передается между абонентами телефонной связи, посредством телефонных факсимильных аппаратов, которые подключены между собой специальной линией телефонной связи и осуществляют передачу устной и письменной информации посредством специально предназначено для этих целей телефонных аппаратов.

2. *Объективная сторона* данного преступления выражается в совершении неправомерных целенаправленных действий направленных на осуществление доступа к телефонным сетям электрической связи и телефонных аппаратов и овладение информацией, которая сообщается между телефонными абонентами.

В части (1) ст. 261[1] УК РМ, законодатель определил, что в качестве преступных действий следует признать именно те неправомерные, т.е. преступные действия, которые повлекли причинение ущерба в крупных размерах. Нанесение ущерба является одним из обязательных элементов данного состава преступления.

Законодатель, однако, не указал, кому должен был быть нанесен ущерб в данном случае: владельцу телефонной сети, собственнику телефонной сети или абоненту который вел и ведет телефонные переговоры либо предает устную, либо письменную информацию по специальным каналам и сетям электрической связи, посредством специальных телефонных аппаратов. Также законодатель не указал, как и каким образом должен быть определен и исчислен нанесенный ущерб в результате осуществления неправомерных

деяний и проникновения в телефонную сеть с целью прослушивания информации передаваемой в результате осуществления телефонных переговоров или передачи письменной информации посредством специальных факсимильных телефонов.

На наш взгляд в данном случае речь идет именно о законной сохранности и конфиденциальности телефонных переговоров, осуществляемых между телефонными абонентами, однако законодатель должен был четко об этом указать в диспозиции вышеназванной нормы права.

Часть (2) ст. 261^1 УК РМ предусматривает и квалифицирующие признаки данного преступления. В качестве таковых законодатель признает:

a) несанкционированный доступ к сетям и/или услугам электросвязи с использованием сетей и\или услуг электросвязи других операторов, совершенный повторно;

b) двумя или более лицами;

c) с нарушением системы защиты телефонных сетей;

d) с использованием специальных технических средств;

e) повлекший причинение ущерба в особо крупных размерах.

Каждый из вышеуказанных пунктов в случае их совершения правонарушителем или правонарушителями образует отдельный состав преступления.

3. *Субъективная сторона* данного преступления характеризуется только прямым умыслом. Цель осуществления несанкционированного доступа к сетям линии электрической связи является овладение устной или письменной информацией и ее незаконное использование в своих корыстных целях.

4. *Субъектом* вышеуказанного преступления является физическое вменяемое лицо, достигшее к моменту совершения преступления 16-ти летнего возраста, а так же юридическое лицо.