Семинар № 9 Правовые средства защиты государственной, служебной и коммерческой тайны

План

1. Понятие государственной тайны и методы ее защиты.

2. Сведения, относимые к государственной тайне.

3. Допуск к государственной тайне.

4. Понятие служебной и коммерческой тайны.

5. Понятие информации. Засекречивание информации.

* 1. Понятие государственной тайны и методы ее защиты.

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Основными методами защиты государственной тайны являются следующие:

1. Скрытие — это один из наиболее общих и широко приме­няемых методов защиты информации. B основе своей он является реализацией на практике одного из основных организационных принципов защиты информации — максимального ограничения числа лиц, допускаемых к секретам. Реализация этого метода дос­тигается обычно путем:

* засекречивания информации, т.е. отнесение ее к секретной или конфиденциальной информации различной степени секретности и ограничение в связи с этим доступа к этой;
* устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

2. Ранжирование как метод защиты информации включает:

* деление засекречиваемой информации по степени секрет­ности;
* регламентацию допуска и разграничение доступа к защищаемой информации, т.е. предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им кон­кретной информации и на выполнение отдельных операций

Ранжирование есть частный случай метода скрытия: пользова­тель не допускается к информации, которая ему не нужна для вы­полнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

3. Дезинформация — один из методов защиты информации, за­ключающийся в распространении заведомо ложных сведений отно­сительно истинного назначения каких-то объектов и изделий, дей­ствительного состояния какой-то области государственной деятель­ности.

4. Дробление представляет собой расчленение информации на части с таким условием, что знание какой-то одной части инфор­мации не позволяет восстановить всю картину, всю техно­логию в целом. Применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве некоторых товаров народного потребления.

5. Страхование как метод защиты информации пока еще только получает признание. Сущность его сводится к тому, чтобы защи­тить права и интересы собственника информации или средства ин­формации как от традиционных угроз (кражи, стихийные бедст­вия), так и от угроз безопасности информации, а именно: защита информации от утечки, хищения, модификации (подделки), разру­шения и др.

6. Морально-нравственные методы играют очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапли­вающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой ин­формации или по его вине соперник получает возможность несанк­ционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предпо­лагают прежде всего воспитание сотрудника, допущенного к секре­там, т.е. проведение специальной работы, направленной на форми­рование у него системы определенных качеств, взглядов и убежде­ний, а также обучение сотрудника, осве­домленного в сведениях, составляющих охраняемую тайну, прави­лам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

7. Учет — это также один из важнейших методов защиты ин­формации, обеспечивающий возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные о всех пользователях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объем.

8. Кодирование — метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в руки соперника, а также при обработке и хране­нии информации.

9. Шифрование — это метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппара­туры, направлении письменных сообщений и в других случаях, ко­гда есть опасность перехвата таких сообщений соперником. Шиф­рование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехватив­ший не имеет сведений (ключа) для раскрытия шифра.

* 1. Сведения, относимые к государственной тайне.

Государственную тайну составляют:

1. сведения в военной области:

* о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций;
* о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации.

1. сведения в области экономики, науки и техники:

* о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники;
* об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства.

1. сведения в области внешней политики и экономики:

* внешнеполитической, внешнеэкономической деятельности Российской Федерации
* о финансовой политике в отношении иностранных государств

1. сведения в области разведывательной, контрразведывательной и [оперативно-розыскной деятельности](https://www.consultant.ru/document/cons_doc_LAW_373004/574645347b3645521c0fde090a627aac2857bf2a/#dst100112), а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

* о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
* о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;
* о методах и средствах защиты секретной информации;
* об организации и о фактическом состоянии защиты государственной тайны;
* о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности;
* о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.
  1. Допуск к государственной тайне

Допуск к государственной тайне регламентируется [законом РФ от 21.07.1993 N 5485-1 (ред. от 09.03.2021) "О государственной тайне"](https://www.consultant.ru/document/cons_doc_LAW_2481/).

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

* принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
* согласие на частичные, временные ограничения их прав в соответствии со [статьей 24](https://www.consultant.ru/document/cons_doc_LAW_378813/5ce6f5340d70927cf5bbf192db2e7a9aa5b8643a/#dst100226) настоящего Закона;
* письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
* определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных настоящим Законом;
* ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;
  1. Понятие служебной и коммерческой тайны.

Разница между этими 2 понятиями заключается в следующем:

* Понятие «служебная тайна» часто применяется к деятельности государственных и муниципальных органов, их должностных лиц и рядовых сотрудников. Под ней подразумеваются данные, тайный характер которых обусловлен интересами службы.
* Информация, относящаяся к коммерческой тайне, несет в себе коммерческую ценность, т. е. с ее помощью обладатель может получить коммерческую выгоду.

Правовая охрана служебной и коммерческой тайны осуществляется в соответствии со следующими актами:

* Ст. 139 Гражданского Кодекса Российской Федерации;
* Ст. 10 Закона РСФСР "О конкуренции и ограничении монополистической деятельности на товарных рынках";
* Законом РФ "Об информации, информатизации и защите информации".

Сведения, являющиеся коммерческой и служебной тайной

Информацию, относящуюся к коммерческой тайне, можно сгруппировать по функционально-целевым признакам:

1. Деловая информация (переговоры, контракты, партнеры, переписка).
2. Производственная информация (технологии, ноу-хау).
3. Финансовая информация (источники финансирования, инвестиции).
4. Информация о персонале и его труде (личные дела работников, планы по организационно-штатным мероприятиям, структура подчиненности, не указанная в уставе, система организации труда).
5. Маркетинговая информация (проведенные исследования, стратегия завоевания рынка, реклама).
6. Информация, связанная с научно-техническими разработками, их концепциями, планами введения в производство.
7. Используемые программы, логины и пароли для доступа к ним.
8. Информация о производимом товаре (его структура, характеристика, параметры и т. д.).

**Служебная тайна** включает в себя информацию, которую условно можно разделить на 2 группы:

1. Сведения, связанные с деятельностью должностных лиц. Например, данные предварительного расследования (тайна следствия), планируемые военные учения (военная тайна) и т. п.
2. Информация, полученная госслужащими в результате их деятельности. К примеру, информация, относящаяся к коммерческой тайне.
   1. Понятие информации. Засекречивание информации.

С юридической точки зрения информация – сведения об окружающем мире, протекающих в нем процессах и сообщение о положении дел или о состоянии чего-либо.

В соответствии со ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации» информация - сведения (сообщения, данные) независимо от формы их представления.

Юридические свойства информации:

* Физическая неотчуждаемость, так как отчуждение информации заменяется передачей прав на ее использование.
* Обособленность – для включения в оборот информация используется в виде символов и знаков и таким образом она обособляется и существует отдельно от производителя.
* Двуединство информации и носителя, т.е. понимание информации как вещи на материальном носителе.
* Распространяемость и тиражирование.
* Организационная форма информации – документ.

Засекречивание информации — это совокупность организационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на рас­пространение и использование информации в интересах ее собст­венника (владельца).

Основные принципы засекречивания информации.

1. Законность засекречивания информации. Она заключается в осуществлении его строго в рамках действующих законов и других подзаконных нормативных актов. Отступление от этого принципа может нанести серьезный ущерб интересам защиты информации, интересам личности, общества и государства, в частности, незакон­ным сокрытием от общества информации, не требующей засекре­чивания, или утечкой важной информации.

2. Обоснованность засекречивания информации. Путем экспертной оценки устанавливается целесообразность засекречивания конкрет­ных сведений и вероятных экономических или иных последствий этого акта, причем делается это исходя из баланса жизненно важ­ных интересов личности, общества и государства. Неоправданно засекречивать информацию, вероятность раскрытия которой пре­вышает возможность сохранения ее в тайне.

3. Своевременность засекречивания информации. Это означает ус­тановление ограничений на распространение секретных сведений с момента их получения (разработки) или заблаговременно.

4. Подчиненность ведомственных мероприятий по засекречиванию информации общегосударственным интересам.

При засекречивании информации решается вопрос не просто об отнесении ее к секретной, конфиденциальной или несекретной, но и о том, какой она должна быть степени секретности,  т.е. решается вопрос об уровне ее защиты.

По Закону РФ «О государственной тайне» правом утверждать перечень сведений, отнесенных к государственной тайне, а также перечень должностных лиц органов государственной власти и управления, имеющих эти полномочия, наделен Президент РФ.

Существуют несколько организационно-правовых форм, в рамках которых осуществляется засекречивание информации, относимой к государственной тайне. Они могут существовать как в «чистом» виде, так и включать в себя элементы других видов форм. Правиль­ный выбор формы может существенно влиять на решение вопросов засекречивания информации: в рамках какой методологии засекре­чивания формируется система критериев определения, затем степе­ни секретности информации.

Существуют следующие основные формы засекречивания ин­формации:

* перечневая форма;
* система первоначального и производного засекречивания;
* программно-целевой подход к засекречиванию информации.

Практические задания

I. Тесты

1. Перечень сведений отнесенных к государственной тайне утверждается

1. Президентом РФ
2. Председателем Правительства РФ
3. Директором Федеральной службы безопасности
4. руководителем организации

2. Перечень сведений, составляющих коммерческую тайну, утверждается

1. Президентом РФ
2. Председателем Правительства РФ
3. Директором Федеральной службы безопасности
4. руководителем организации

3. Закон "Об авторском праве и смежных правах" защищает права

1. исполнителей (актеров, певцов и т.д.)
2. производителей фонограмм
3. организации эфирного и кабельного вещания
4. всех лиц, перечисленных в остальных пунктах

4. Какой законодательный акт содержит сведения по защите коммерческой тайны?

1. Закон "Об авторском праве и смежных правах"
2. Закон "О коммерческой тайне"
3. Патентный закон
4. Закон "О правовой охране программ для ЭВМ и баз данных"

5. К информации ограниченного доступа не относится

1. государственная тайна
2. размер золотого запаса страны
3. персональные данные
4. коммерческая тайна

II. Задачи

В одной из газет появилось сообщение о том, что популярный телеведущий получил ссуду в размере 1 млн 200 тыс. рублей на строительство. Он открыл депозитный счет в одном из отделений коммерческого банка. После публикации данного материала в районный суд поступило исковое заявление от телеведущего к коммерческому банку о возмещении морального вреда и о разглашении коммерческой тайны.

Проанализируйте ситуацию с позиции нарушений законодательства.

Разберите ситуацию. Подлежат ли ответственности банк и газета?

Был ли нарушен редакцией газеты закон «О средствах массовой информации», а банком ГК РФ – закон «О банках и банковской деятельности»?

ГК РФ Статья 857. Банковская тайна.

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены [законом](https://www.consultant.ru/document/cons_doc_LAW_359091/d4984b968b67d38939333aa51c71bcb189047fbb/#dst100124). Государственным органам и их должностным лицам, а также иным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены [законом](https://www.consultant.ru/document/cons_doc_LAW_372893/5583e2cafb06542e33c725aa32666e8ab89b1cdc/#dst100524).

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Согласно этой статье банк нарушил закон и выдал газете данные о размере банковского вклада. Банк разгласил эти сведения и клиент вправе потребовать возмещения причиненных убытков от банка

Согласно [закону РФ "О средствах массовой информации"](https://www.consultant.ru/document/cons_doc_LAW_1511/) в статье 49 Обязанности журналиста сказано, что журналист обязан:  получать согласие (за исключением случаев, когда это необходимо для защиты общественных интересов) на распространение в средстве массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей;

В статье 24 Конституции РФ закреплено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Согласно Федеральному закону «О персональных данных» обработка персональных данных, в том числе и сведений о частной жизни лица, включая их сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, может осуществляться только с согласия субъекта персональных данных.

Таким образом не получив согласие от популярного телеведущего на распространение данных газета нарушает вышеприведенные статьи.

III. Темы докладов

1. Юридическая ответственность за разглашение охраняемой законом информации.

Согласно ФЗ «Об информации, информационных технологиях и защите информации» понятие «конфиденциальная информация» характеризируется, как сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их правообладателя.

За разглашение конфиденциальной информации, утрату носителей конфиденциальной информации и нанесение вследствие этих действий ущерба предприятию (работодателю) виновные лица привлекаются к дисциплинарной, материальной, административной или уголовной ответственности.

Перечень сведений, составляющих государственную тайну указан в ст. 5 Закона РФ «О государственной тайне». В основном к ним относятся определенные сведения из военной области, области экономики, науки и техники, внешней политики и экономики, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Работник за разглашение конфиденциальной информации (при отсутствии в действиях такого работника состава преступления) несет дисциплинарную ответственность. Кроме того, в соответствии со ст.238 ТК РФ с сотрудника может быть взыскан прямой действительный ущерб, например стоимость носителя информации. Трудовой кодекс помимо включения в трудовой договор условия о неразглашении охраняемой законом тайны предусматривает возможность увольнения работника за разглашение государственной, коммерческой, служебной или иной тайны. Кроме того, ст. 243 ТК РФ устанавливает полную материальную ответственность работника за разглашение сведений, составляющих служебную, коммерческую или иную охраняемую законом тайну в случаях, предусмотренных федеральным законом. Доказать величину убытков достаточно сложно. И стоимость самой утраченной конфиденциальной информации, и размер упущенной выгоды являются величиной достаточно условной. Кроме того, рассматривая претензии организаций к работникам, суды часто встают на сторону персонала. Возможно и уголовное преследование лиц, разгласивших конфиденциальную информацию. Однако взысканные штрафы будут направлены в бюджет, а пострадавшая организация может рассчитывать только на моральное удовлетворение.

1. Проблемы правового регулирования Интернета.

Отсутствие нормативных правовых актов, регулирующих непосредственно отношения в сети Интернет, как и возможность их эффективного применения, уже сейчас оказывает негативное влияние на развитие общественных отношений (например, в области авторских прав, персональных данных, интернет-торговли, информационной безопасности и др.).

Основными проблемами в сети Интернет, нуждающимися в скорейшем нормативно-правовом урегулировании, являются:

1. Распространение экстремистских материалов в сети Интернет.

2. Проблемы, связанные с защитой прав интеллектуальной собственности в сети Интернет.

3. Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

4. Защита персональных данных.

5. Правовое регулирование электронной торговли в сети Интернет.

6. Пропаганда, незаконная реклама наркотических средств и психотропных веществ.

7. Незаконное распространение порнографических материалов в сети Интернет.

8. Клевета в сети Интернет.

9. Мошенничество в сети Интернет

Распространение экстремистских материалов в сети Интернет.

Сеть Интернет предоставляет членам экстремистских движений и групп возможность отстаивать и пропагандировать свою идеологию в информационных ресурсах интернета, где сосредоточено огромное количество пользователей. Особенно легко воздействию данной проблемы подвергаются подростки. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» устанавливает недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности (ст. 12), ответственность за распространение экстремистских материалов (ст. 13). Для решения данной проблемы необходимо усовершенствовать нормативно-правовую базу, разграничить компетенции правоохранительных органов в сфере борьбы с терроризмом и экстремизмом в сети Интернет, ужесточить меры наказания за совершение преступлений данного характера.

Проблемы, связанные с защитой прав интеллектуальной.

Нелегальное распространение фильмов, телепередач и иных видеороликов, а также музыкальных произведений, книг и программных продуктов в сети Интернет достигает гигантских масштабов, так как сеть Интернет предоставляет достаточно возможностей для фактически бесконтрольного воспроизведения и распространения таких объектов.  За нарушение авторских и смежных прав, а также изобретательских и патентных прав предусматривается гражданско-правовая, административная и уголовная ответственность. Согласно Гражданскому кодексу РФ защита исключительных прав осуществляется в соответствии со ст. 1252, в ст. 1253.1 говорится, что «информационный посредник несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных настоящим Кодексом, при наличии вины с учетом особенностей, установленных пунктами 2 и 3 настоящей статьи». В Уголовном кодексе — ст. 146, 147. Данному вопросу посвящена также ст. 15.2 Федерального закона «Об информации, информационных технологиях и о защите информации», где рассматривается порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав.

Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

Вопросы, связанные с правовым регулированием исключительных прав на сетевой адрес, приобретают всё более широкие границы. На данный момент судебные споры, касающиеся доменных имен, являются наиболее частыми в судебной практике, особенно в странах Запада. Возможность свободного выбора доменного имени породило противоправное явление - кибер-сквоттинг, означающее регистрацию доменных имен, совпадающих или сходных со средствами индивидуализации, с их последующим недобросовестным использованием как для собственных коммерческих целей, так и с целью предложения к продаже самим правообладателям средств индивидуализации. Далеко не всегда в этом случае владельцы товарных знаков добивались защиты своих прав и устранения нарушений. Суд отказывал правообладателю в защите прав со ссылкой на отсутствие законодательного регулирования отношений, связанных с наименованием доменов в сети Интернет, а также на то, что доменное имя не является ни товаром, ни услугой, поэтому не подпадает под действие Закона «О товарных знаках».

Защита персональных данных в сети Интернет.

Недостаточное обеспечение защиты персональных данных субъектов РФ является одной из распространенных проблем в виртуальной среде российского сегмента сети Интернет. Федеральный закон «О персональных данных» не решает большинства юридических проблем, даже дополнение Федерального закона «Об информации, информационных технологиях и о защите информации» статьей 15.5, в которой указывается порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, оставляет данный вопрос открытым и актуальным.

Правовое регулирование электронной торговли в сети Интернет.

К проблематичным вопросам в сфере электронной торговли в интернете относятся вопросы заключения контрактов посредством сети Интернет, вопросы недобросовестной рекламы, спама, проблема налогообложения предпринимательства в сети Интернет. Крайне важной в интернет-праве является в настоящее время проблема ответственности за качество информации, предоставляемой продавцом в рамках электронной торговли. Практика показывает, что приобретение товаров через сеть Интернет сопряжено со многими возможными конфликтными ситуациями, которые следует учитывать как продавцам, так и покупателям, т.е. всем субъектам (участникам) отношений в сети Интернет.

Есть проблемы, связанные с деятельностью коммерческих онлайновых компаний. Эти проблемы можно подразделить на следующие:

1) регулирование содержания (вредное и незаконное);

2) соблюдение авторских и смежных прав в условиях технически легкого копирования любой информации, представленной в цифровом виде;

3) вопросы формирования киберэкономики (электронные деньги, реклама, маркетинг, электронные публикации, электронные контракты, налог на передачу информации);

4) информационная безопасность, понимаемая в широком смысле как безопасность жизненно важных для общества систем управления: транспортом, войсками, хозяйством крупных городов и т.п.

Незаконное распространение порнографических материалов в сети Интернет.

Отметим, что эротическая и порнографическая продукция в большинстве стран мира не запрещена, а ограничена. Данные ограничения касаются:

1) времени публичного показа данной продукции;

2) места ее расположения;

3) вовлечения несовершеннолетних.

Основная цель введения этих ограничений — сделать эротические и порнографические материалы недоступными для несовершеннолетних, так как данный вид продукции оказывает травмирующее воздействие на психику подростков (ст. 5 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Клевета в сети Интернет.

В сети Интернет имеется возможность, которая позволяет распространять информацию, дискредитирующую граждан, субъекты отношений в сети Интернет, сохраняя при этом анонимность.

Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети Интернет, гражданин вправе требовать удаления соответствующей информации, а также опровержения указанных сведений способом, обеспечивающим доведение опровержения до пользователей сети Интернет (ч. 5 ст. 152 Гражданского кодекса РФ). По Уголовному кодексу РФ в соответствии с ч. 2 ст. 128.1 клевета наказывается штрафом.

Мошенничество в сети Интернет.

Мошенничество в соответствии со ст. 159 Уголовного кодекса РФ — «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». На данный момент существует огромное количество различных видов мошенничества в сети Интернет, следует учитывать и то, что с течением времени появляются все новые виды мошенничества.

Выделим те из них, которым наиболее часто подвергаются пользователи Сети:

* Интернет-попрошайничество — один из наиболее известных видов мошенничества в Сети, которое выражается в просьбе пожертвовать некоторую сумму денежных средств под различными предлогами, например от имени благотворительных фондов;
* Сайты-подделки — внешне не отличаются от оригинальных сайтов. Однако сайты-подделки популярных социальных сетей создаются с целью выманивания денежных средств или взлома аккаунтов, с последующей рассылкой писем, содержащих ссылки на вредоносные программы - спама;
* Программы-блокеры — созданы для проникновения в систему и блокирования доступа к ней. Для разблокировки системы пользователю требуется, как пример, отправить платное sms-сообщение;
* Фишинг является также одним из наиболее распространенных видов мошенничества, его целью является получение доступа к конфиденциальным данным пользователей (логинам и паролям). Осуществляется данный вид интернет-мошенничества путем проведения массовых рассылок электронных писем от известных пользователю представителей.

Решение данных проблем, несомненно, требует правового государственного регулирования, а также межгосударственного сотрудничества в борьбе с сетевой преступностью, терроризмом и экстремизмом в сети Интернет. Но большее внимание следует уделить проблеме предупреждения преступлений в сети Интернет. При подключении к сети Интернет пользователь порой не получает никакой информации об устройстве Сети, о мерах защиты данного соединения и тем более о том, какие меры предосторожности стоит соблюдать. Необходимо разработать программы, программные продукты и обеспечение по защите от возможных опасностей, связанных с использованием сети Интернет. В особенности это важно и актуально для тех пользователей сети Интернет, которые только начинают ее осваивать, особое внимание необходимо уделить несовершеннолетним пользователям. Законодательство Российской Федерации отражает постепенное формирование правовой базы регулирования отношений в данной сфере деятельности, однако стремительное развитие информационно-телекоммуникационных технологий, в особенности сети Интернет, не позволяет своевременно обновлять законодательную базу, вносить изменения и дополнения.