# Введение.

В условиях, когда планета Земля становится единым домом человечества, многие противоречия, конфликты, проблемы могут перерасти локальные рамки и приобрести глобальный общемировой характер.

# Сегодня важно сознавать неразрывную связь природы, техники и общества, которое носит взаимный характер.

# В данной работе я осветил две темные стороны человеческой деятельности. Это экологические и компьютерные преступления. Первые, если не держать контроль за ними, и не стремиться искоренить их приведу к тому, что на земле скоро не будет нормальной земли и чистой воды, будут истреблены многие животные. Это так называемая глобальная экологическая катастрофа. Вторые могут привести в конечном итоге к информационной катастрофе, что в рамках нашего уклада жизни просто непредставимо. Ведь практически все в нашей жизни управляется с помощью компьютера или через связь с ним. Не того компьютера, который стоит на столе почти у каждого из нас дома, а самых разнообразных машин, объединенных одним словом компьютер.

Но чтобы этого всего добиться, нужно, прежде всего, знать правовые основы, иметь понятие как бороться с данной проблемой.

Итак, начнем с экологических преступлений.

# Юридическая ответственность за нарушения экологического законодательства

В соответствии со ст.ст.4 Закона «Об охране окружающей природной среды» охране от загрязнения, порчи, повреждения, истощения, разрушения на территории Российской Федерации и республик в составе Российской Федерации подлежат следующие объекты природопользования:

* естественные экологические системы, озоновый слой атмосферы;
* земля, ее недра, поверхностные и подземные воды, атмосферный воздух,
* леса и иная растительность, животный мир, микроорганизмы, генетический фонд,
* природные ландшафты.

Особой охране подлежат государственные природные заповедники, природные заказники, национальные природные парки, памятники природы, редкие или находящиеся под угрозой исчезновения виды растений и животных и места их обитания.

**За экологические правонарушения должностные лица и граждане несут дисциплинарную, административную, либо уголовную, гражданско-правовую, материальную, а предприятия, учреждения, организации — административную и гражданско-правовую ответственность в соответствии с настоящим Законом, иными законодательными актами Российской Федерации и республик в составе Российской Федерации.**

Данное определение, содержащее основные отличительные признаки экологического правонарушения, но имеет ряд недостатков. Так, в нем указаны не все признаки правонарушения; перечислены не все социальные ценности, составляющие предмет экологических правоотношений, которым причиняется вред; в качестве систематизирующего признака взяты последствия, а не объект правонарушения.

Состав экологического правонарушения включает в себя четыре элемента: **объект, объективная сторона, субъективная сторона, субъект**.

**Объект** представляет собой совокупность общественных отношений по охране окружающей природной среды, рациональному использованию ее ресурсов и обеспечению экологической безопасности.Природная среда в целом и ее отдельные компоненты) являются предметом правонарушения.

Для **объективной стороны** экологического правонарушения характерно нарушение путем действия или бездействия общеобязательных правил природопользования и охраны окружающей природной среды; причинение вреда экологическим интересам личности, общества или государства либо создание реальной опасности причинения такого вреда; наличие причинной связи между экологически опасным деянием и причиненным вредом.

С **субъективной стороны** могут иметь место обе формы вины: *умышленная и неосторожная*.

*Умысел* может быть *прямым и косвенным*, а н*еосторожность* — в виде *небрежности или самонадеянности* (легкомыслия).

**Субъектами** экологического правонарушения могут быть как физические, так и юридически лица, включая хозяйствующих субъектов различных форм собственности и подчиненности, а также иностранные организации и граждане.

# Экологические преступления общего характера

— нарушение правил охраны окружающей среды при производстве работ (ст. 246);

— нарушение правил обращения с экологически опасными веществами и отходами (ст. 247);

— нарушение правил безопасности при обращении с микробиологическими или другими биологическими агентами или токсинами (ст. 248);

— нарушение законодательства РФ о континентальном шельфе и об исключительной экономической зоне РФ (ст. 253);

— нарушение режима особо охраняемых природных территорий и природных объектов (ст. 262).

# Специальные экологические преступления

*1) преступления, посягающие на общественные отношения в области охраны и рационального использования земли, недр и обеспечения экологической безопасности*:

— порча земли (ст. 254);

— нарушение правил охраны и использования недр (ст. 255);

*2) преступления, посягающие на общественные отношения в области охраны и рационального использования животного мира(фауны):*

— незаконная добыча водных животных (ст. 256);

— нарушение правил охраны рыбных запасов (ст. 257);

— незаконная охота(ст. 258);

— нарушение ветеринарных правил (ч. 1 ст. 249);

— уничтожение критических местообитаний для организмов, занесенных в Красную книгу Российской Федерации (ст. 259);

*3) преступления, посягающие на общественные отношения по охране и рациональному использованию растительного мира (флоры):*

— незаконная порубка деревьев и кустарников (ст. 260);

— уничтожение или повреждение лесов (ст. 261);

— нарушение правил, установленных для борьбы с болезнями и вредителями растений (ч. 2 ст. 249);

— незаконная добыча водных растений (ст. 256).

*4) преступления, посягающие на объективные отношения по охране и рациональному использованию вод и атмосферы, а также обеспечению экологической безопасности:*

— загрязнение вод (ст. 250);

— загрязнение морской среды (ст. 252);

—загрязнение атмосферы (ст. 251).

Компьютерные преступления

В нашей стране не законодательном уровне выделено три основных вида компьютерных преступлений:

1. Неправомерный доступ к компьютерной информации; Статья 272. УКРФ
2. Создание, использование и распространение вредоносных программ для ЭВМ; Статья 273 УКРФ;
3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Статья 274 УКРФ.

На мой взгляд наиболее опасным является первое, так как остальные совершаются как правило именно для получения этой самой информации нелегальным путем.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Несанкционированный доступ к информации, хранящейся в компьютере.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, использованием информации, оставшейся после решения задач, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры. Гудини информационных сетей. Для некоторых взлом и копание в информации развлечение, для других бизнес. Они могут ночами биться в закрытые двери (шлюзы) сетей или компьютеров конкретных людей перебирая простые слова в качестве пароля. И это не так глупо как кажется (по крайней мере, было до недавнего времени). Есть еще несколько довольно простых и эффективных способов незаконного подключения к удаленным компьютерам но я пишу не учебник для хакеров, поэтому приводить их не буду а продолжу доклад.

Ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему. Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники, например, отчисляют на свой счет определенную сумму с каждой операции. Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен тысяч, а иногда и миллионов команд. Поэтому "троянский конь" из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого.

Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Интересен случай использования "троянского коня" одним американским программистом. Он вставил в программу компьютера фирмы, где работал, команды, не отчисляющие деньги, а не выводящие на печать для отчета определенные поступления. Эти суммы, особым образом маркированные, "существовали" только в системе. Вульгарным образом украв бланки, он заполнял их с указанием своей секретной маркировки и получал эти деньги, а соответствующие операции по-прежнему не выводились на печать и не могли подвергнуться ревизии.

Разработка и распространение компьютерных вирусов. "Троянские кони" типа сотри все данные этой программы, перейди в следующую и сделай то же самое", обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Каковы способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве "средства передвижения". То есть дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда "здоровая" дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это копирование программ, что является обычной практикой у пользователей персональных ЭВМ.

Справедливости ради следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

Подделка компьютерной информации.

Повидимому этот вид компьютерной преступности является одним из

наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов

выборов, голосований, референдумов и т. п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

Здесь можно вспомнить, например, случай с исчезновением 352 вагонов на нью-йоркской железной дороге в 1971 году. Преступник воспользовался информацией вычислительного центра, управляющего работой железной дороги, и изменил адреса назначения вагонов. Нанесенный ущерб составил более миллиона долларов.

Служащий одного нью-йоркского банка, изменяя входные данные, похитил за 3 года 1,5 миллиона долларов. В Пеисильвании (США) клерк инесколько рабочих крупного мебельного магазина, введя с терминала фальшивые данные, украли товаров на 200 тыс. долларов.

Хищение компьютерной информации.

Если "обычные" хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изьятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный

предмет уголовно-правовой охраны.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является "средством" достижения цели. Здесь можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными рекомендации по выбору оптимального варианта действий преступника.

Классическим примером служит дело собственника компьютерной службы, бухгалтера по профессии, служившего одновременно бухгалтером пароходной компании в Калифорнии (США), специализировавшейся на перевозке овощей и фруктов. Он обнаружил пробелы и деятельности ревизионной

службы компании и решил использовать этот факт. На компьютере своей службы он смоделировал всю бухгалтерскую систему компании. Прогнав модель вперед и обратно, он установил, сколько фальшивых счетов ему необходимо и какие операции следует проводить.

Он организовал 17 подставных компаний и, чтобы создать видимость реальности ситуации, обеспечил каждую из них своим счетом и начал денежные операции. Модель бухгалтерского баланса подсказала ему, что при имеющихся пробелах в ревизионной службе, 5%-ное искажение не будет заметно, Его действия оказались настолько успешными, что в первый год он похитил 250 тыс. долларов без какого-либо нарушения финансовой деятельности компании. К тому времени, когда увеличенные выплаты вызвали подозрение -- даже не у самой компании, а у ее банка, -- сумма хищения составила миллион долларов .

Другой вид преступлений с использованием компьютеров получил название "воздушный змей".

В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз ("воздушный змей" поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Дело этого типа имело место в Лондоне. Группа мошенников объединилась с несколькими специалистами по компьютерам. Они обзавелись микрокомпьютером, сделали моделирующую программу и начали действовать по указанию из "штаб-квартиры", куда звонили по телефону и получали указания в соответствии с рекомендациями модели. Все шло блестяще и "змей" уже забрался чрезвычайно высоко, но тут произошел сбой в компьютере. Дублирующего компьютера не предусмотрели, и "змей" рухнул.

Скотлэнд Ярд за несколько дней арестовал всех мошенников. След естественным образом привел к "штаб-квартире", где специалисты по компьютерам, забыв об отдыхе, пытались наладить работу компьютера .

Тем же самым способом служащий банка в Лос-Анджелесе со своими сообщниками, которые давали поручения о переводе, похитил 21,3 млн. долларов. Здесь технология запуска "змея" была более четкой. По указаниям моделирующей программы открывалось большое количество новых счетов, размер переводимых сумм менялся и т. д.

После всего сказанного хотелось бы наконец перейти на правовую основу всего выше сказанного.

Мы будем различать на законодательном уровне две группы мер:

* меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
* направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но мне хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

**Правовые акты общего назначения, затрагивающие вопросы информационной безопасности**

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 – право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 – "Преступления в сфере компьютерной информации" – содержит три статьи:

статья 272. Неправомерный доступ к компьютерной информации;

статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;

статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая – с вредоносным ПО, третья – с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Процитируем статью 19.

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

***Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...***

О текущем состоянии российского законодательства в области информационной безопасности

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет и, увы, не предвидится. Сейчас бессмысленно задаваться вопросом, чего не хватает российскому законодательству в области ИБ, это все равно что интересоваться у пунктирного отрезка, чего тому не хватает, чтобы покрыть всю плоскость. Даже чисто количественное сопоставление с законодательством США показывает, что наша законодательная база явно неполна.

Справедливости ради необходимо отметить, что ограничительная составляющая в российском законодательстве представлена существенно лучше, чем координирующая и направляющая. Глава 28 Уголовного кодекса достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.

А в заключении своего выступления хотелось бы отметить, правовая сторона этого вопроса не готова к действию. А следовательно доказать что-либо бывает очень трудно, по крайней мере в нашей стране. Да и законодательный процесс, по моему мнению, не догонит информационный прогресс, а следовательно мы никогда не будем готовы полностью к борьбе с компьютерными преступлениями. Всегда будут находиться способы обойти закон в свою пользу.

Что же касается экологических преступлений, то здесь все не так страшно. И способов борьбы больше и видов преступлений меньше. Другое дело находились бы люди, которые это все делают не только из-за денег, но и свою страну немного смогут защитить. От себя самих же. Ведь не трудно же пронести выкуренную сигарету до урны, а не бросать ее под ноги. Много еще таких примеров, приводить не буду, времени нет. Хотелось бы вспомнить один старый принцип: «Чисто не там, где убирают, а там, где не мусорят».

Спасибо за внимание.