**ПОНЯТИЕ «КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ»**

Компьютерные преступления многоаспектны и потому могут относиться к самым различным видам преступных посягательств и отличаться не только по объекту посягательства, но и по способам, мотивам и другим признакам. Единственным основанием отнесения преступления к данной категории является наличие средства вычислительной техники как носителя охраняемой законом компьютерной информации, выступающего в качестве объекта или орудия совершения преступления. Поэтому криминалистическая характеристика компьютерных преступлений отличается определенной спецификой.

Стержневой основой компьютерных преступлений являются предусмотренные уголовным законом общественно опасные деяния, посягающие на безопасность компьютерной информации и орудий ее обработки, выделенные в специальную главу № 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации.

Под компьютерной информацией законодателем при этом понимается информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети, т. е. машинная информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной восприятию ЭВМ, или передающаяся по каналам электросвязи посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство, либо на управляющий датчик оборудования.

Данная глава предусматривает деяния, в которых предметом посягательства является СВТ как информационная структура и материальный носитель информации, а именно:

- неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272 УК РФ);

- создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами (ст. 273 УК РФ);

- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим к ним доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (ст. 274 УК РФ).

В соответствии со ст. 2 Закона «Об информации, информатизации и защиты информации», под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация обязательно должна быть чужой для преступника и защищенной от неправомерного использования.

Следует подчеркнуть, что конфиденциальная информация - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ст. 2 Закона «Об информации, ...») - всегда будет чужой для лица, не имеющего к ней допуска. При этом, законодательством России ограничивается доступ к следующим основным видам информации, которые одновременно подлежат обязательной защите, а именно:

- сведения, отнесенные к государственной тайне соответствующим Федеральным Законом «О государственной тайне», под которыми на основании ст. 5 понимается информация в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности России (Закон РФ «О государственной тайне» и ст. ст. 275, 276, 283, 284 УК РФ);

- сведения, передаваемые путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ и ст. 138 УК РФ);

- сведения, отнесенные к служебной, коммерческой или банковской тайне;

- в соответствии со ст. 139 Гражданского кодекса России, информация составляет служебную или коммерческую тайну в случае, когда она 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;

- в соответствии со ст. 183 Уголовного кодекса России незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну подлежат уголовной ответственности;

- сведения, являющиеся объектом авторских и смежных прав (Закон РФ «Об авторском праве и смежных правах» и ст. 146 УК РФ);

- сведения, имеющие статус персональных данных, под которыми в соответствии со ст. 11 Федерального Закона «Об информации, информатизации и защиты информации» понимается информация о гражданах, т. е. сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, - касающиеся тайны усыновления (удочерения) - ст. 155 УК РФ; нарушения неприкосновенности частной жизни (личной или семейной тайны) - ст.137 УК РФ; отказа в предоставлении гражданину информации, непосредственно затрагивающей его права и свободы, либо предоставление гражданину неполной или заведомо ложной информации - ст. 140 УК РФ.

Последствия неправомерного использования информации могут быть различные, например: нарушение неприкосновенности интеллектуальной собственности, разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации, различные виды нарушений нормальной деятельности предприятий, учреждений, организаций и целых отраслей и т. д.

В то же время физическое повреждение или уничтожение исключительно аппаратно-технического СВТ, незаконное завладение им как предметом, обладающим материальной ценностью, квалифицируется как посягательство на чужое имущество по ст. 158 - 168 главы 21 «Преступления против собственности» УК РФ, тогда как преступления в сфере компьютерной информации, условно говоря, сопряжены с посягательством на иной предмет - информацию, сосредоточенную внутри этих СВТ и одновременно являющихся ее материальными носителями в виде разнообразных карт, лент, дисков, микросхем, кристаллов и т. д.

Возможен также вариант, когда СВТ одновременно выступает в качестве как предмета, так и орудия совершения преступления, например, физическое повреждение аппаратно-технического СВТ (экрана монитора, дисковода, принтера и т. д.) с помощью вредоносной программы, нестандартного физического носителя машинной информации либо запрограммированного специального технического устройства. В этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и в сфере компьютерной информации, поскольку страдают два объекта уголовно-правовой охраны, равно как и в других подобных случаях.

Аппаратно-техническое средство электронно-вычислительной техники как орудие совершения преступления рассматривается наравне с такими, как оружие, транспортное средство, любое техническое приспособление. В этом смысле его использование имеет прикладное значение, например, для хищения, шпионажа, убийства, легализации денежных средств, уклонения от уплаты платежей и налогов, подделки документов, незаконного распространения порнографических материалов, изготовления поддельных кредитных либо иных расчетных карт, нарушения правил безопасности движения транспорта и международных полетов, разглашение государственной тайны и т. д. Поэтому такого рода действия самостоятельных составов преступлений не образуют, а квалифицируются по различным статьям Уголовного кодекса.

При использовании компьютерной информации в качестве средства совершения другого преступления, она сама становится предметом общественно опасного деяния в связи с тем, что невозможно противоправно воспользоваться информацией, хранящейся в ЭВМ, не нарушив при этом ее правовой защиты, т. е. не совершив хотя бы одного из действий, перечисленных в ст. 20 Закона «Об информации, информатизации и защиты информации» РФ, а именно: утечки (неправомерного выхода сведений за пределы контролируемой правообладателем территории), хищения, утраты, искажения, подделки, уничтожения (невозможности восстановления), модификации (существенного видоизменения первоначальной информации без согласия правообладателя, затрудняющее законное пользование информацией), копирования (аутентичного по содержанию частичного или полного воспроизведения оригинала машинной информации в любой форме на физическом носителе без согласия правообладателя), блокирования (создания препятствий к свободному пользованию информации при одновременной сохранности ее исходной формы).

В том случае, если сведения, находящиеся в конкретной ЭВМ, правомерно употребляемые ее законным пользователем не пострадают, то неизбежно подвергнутся ущербу те, с которыми она связанна сетью или через машинные носители информации. Таким образом, ответственность за подобные деяния должна наступать по правилам идеальной совокупности преступлений, например, при совершении хищения с использованием СВТ.

Несмотря на достаточно четкое определение элементов объективной стороны, вопросы квалификации компьютерных преступлений вызывают у следователей известную трудность.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ. ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ

Криминалистическая характеристика компьютерных преступлений отличается от уже известных преступных посягательств определенной спецификой. Основные структурные элементы преступлений данного вида обладают существенным своеобразием. В первую очередь выделяют следующие криминалистически значимые сведения:

- о личности правонарушителя;

- о мотивах и целях его преступного поведения;

- о типичных способах подготовки, совершения и сокрытия преступления;

- о времени, месте и обстановке посягательств.

**Обстановка** совершения компьютерного преступления включает в себя материальные, производственные и социально-психологические факторы среды, в которой происходит преступное деяние. Она способна влиять на формирование всех остальных элементов криминалистической характеристики преступления рассматриваемой категории, определять особенности поведения преступника и потерпевшей стороны.

Наиболее важным компонентом обстановки подготовки, исполнения и сокрытия преступления в данном случае являются специфические условия деятельности потерпевших сторон ( физических и юридических лиц ) и среди них следующие *объективные*:

- вид деятельности или род занятия (сфера деятельности - хозяйственная, коммерческая, управленческая, производственная, информационная, посредническая, финансовая, топливно-энергетическая, транспортная, услуг и т. д.);

- форма собственности предприятия или физического лица, правовой режим отдельных видов имущества, в т. ч. информации и информационных ресурсов;

- назначение и структура организации производственного процесса, характер потребляемых ресурсов и выпускаемой продукции (в т. ч. и интеллектуальной);

- система учета и отчетности;

- кадровое и материально-техническое обеспечение;

- вид используемых СВТ, связи и телекоммуникаций, их тактико-технические данные и конструктивное несовершенство;

- погодные условия;

- наличие необходимых помещений и оборудования;

- порядок отпуска и реализации продукции, ценностей;

- наличие и техническое состояние средств учета, защиты информации, охраны и т. д.

К *субъективным* условиям относятся такие факторы социально-психологического и организационно-управленческого характера как:

- отступление от технологических режимов обработки информации, правил производства, проведения пусконаладочных, ремонтных, регламентных (техническое обслуживание) работ, эксплуатации СВТ, а также учета, хранения, распределения и расходования ценностей;

- несовершенство этих правил;

- отсутствие или несовершенство средств защиты информации;

- нарушение правил работы с охраняемой законом компьютерной информацией;

- необоснованность использования СВТ в конкретных технологических процессах и операциях;

- неудовлетворительная организация производственных процессов, наличие одновременно ручных и автоматизированных этапов обработки документов;

- психологически неправильные межличностные взаимоотношения руководителей с подчиненными и другими работниками и т. д.

Субъективные факторы могут существенно влиять на обстановку совершения компьютерных преступлений и определенным образом формировать ее. Существенным компонентом криминалистической характеристики преступлений, связанных с использованием СВТ, являются **сведения об особенностях личности правонарушителя.**

На жаргонном языке компьютерных правонарушителей называют «хэкерами», «крэкерами» и «фрэкерами». Эти названия произошли от соответствующих английских слов «hacker», «cracker» и «phracker», первое из которых обозначает пользователя ЭВМ, системы ЭВМ или их сети, занимающегося несанкционированным поиском способов получения неправомерного доступа к СВТ и охраняемой законом компьютерной информации, второе - пользователя ЭВМ, системы ЭВМ или их сети, занимающегося «взломом» (модификацией, блокированием, уничтожением) программно-аппаратных средств защиты компьютерной информации, охраняемых законом, третье - субъекта, специализирующегося на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации. Данные лица обычно обладают достаточно высокими специальными познаниями и практическими навыками в области новых компьютерных технологий. Как правило, это увлеченные компьютерной техникой школьники, студенты и молодые специалисты, совершенствующиеся на этом виде деятельности.

По последним данным, хэкеры в России объединены в региональные группы, издают свои электронные средства массовой информации (газеты, журналы, электронные доски со срочными объявлениями), проводят электронные конференции, имеют свой жаргонный словарь, который постоянно пополняется и распространяется с помощью компьютерных бюллетеней. В таких « литературных» источниках имеются все необходимые сведения для повышения мастерства начинающего правонарушителя - методики и конкретные способы совершения и сокрытия компьютерных преступлений от самых простых и до очень изощренных и сложных. Российские хэкеры тесно контактируют с зарубежными, обмениваются с ними опытом по глобальным телекоммуникационным каналам электросвязи.

Возраст преступников колеблется от 15 до 45 лет. Например, по данным некоторых исследователей, на момент совершения преступления возраст 33% преступников не превышал 20 лет, 13% - старше 40 лет и 54% - 20-40 лет.

Стоит подчеркнуть, что 87% преступников - это служащие предприятий, учреждений и организаций, в которых было совершено преступление.

Характерные **мотивы** и **цели** компьютерных преступлений следующие:

- незаконное получение денег, ценных бумаг, кредита, материальных ценностей, товаров, услуг, привилегий, льгот, квот, недвижимости, топливно-сырьевых и энергетических ресурсов, стратегического сырья;

- уклонение от уплаты налогов, платежей, сборов и т. п.;

- легализация (отмывание) преступных доходов;

- подделка или изготовление поддельных документов, штампов, печатей, бланков, денежных билетов в корыстных целях;

- получение конфиденциальной информации в корыстных или политических целях;

- месть на почве личных неприязненных отношений с администрацией или сослуживцами по работе;

- дезорганизация валютной системы страны в корыстных или политических целях;

- дестабилизация обстановки в стране, территориально-административном образовании, населенном пункте (в политических целях);

- дезорганизация работы учреждения, предприятия или системы с целью вымогательства, устранения конкурента или в политических целях;

- стремление скрыть другое преступление;

- хулиганские побуждения и озорство;

- исследовательские цели;

- демонстрация личных интеллектуальных способностей или превосходства.

**Время совершения преступлений** рассматриваемой категории лишь в относительно редких случаях устанавливается с точностью до дня и очень редко - до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

**Местом совершения компьютерных преступлений** являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в каком-либо технологическом процессе. Следовательно, по делам данной категории мест совершения преступных посягательств может быть несколько, в том числе значительно удаленных друг от друга и расположенных как в разных странах, так и на различных континентах. Последнее возможно по причине практически неограниченного радиуса действия и мобильности электронных средств связи и телекоммуникаций, неотъемлемой частью которых являются СВТ.

Ярким примером этому может служить одно из уголовных дел, расследование которого осуществлялось отечественными правоохранительными органами в тесном контакте с правоохранительными органами США. Возбуждено оно было в отношении В. Левина - гражданина Российской Федерации, 13-ти русских с иностранным подданством, а также гражданина Нидерландов, которые вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих «City Bank of America», расположенному в Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 1994 года, используя электронную компьютерную систему телекоммуникационной связи ИНТЕРНЕТ и преодолев семь рубежей многоконтурной защиты от несанкционированного доступа, с помощью персонального компьютера из офиса АО «Сатурн», находящегося в городе Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих действий преступники осуществили около 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка, находящихся в 10 странах мира - США, Канаде, Мексике, Аргентине, Новой Зеландии, Арубе, Колумбии, Гонконге, Индонезии, Уругвае, на счета лиц, входящих в состав преступной группы и проживавших в 7-ми других странах - США, Финляндии, Израиле, Швейцарии, Германии, России и Нидерландах.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного преступления, является совокупность данных, характеризующих способ его совершения.

Все **способы подготовки, совершения и сокрытия компьютерных преступлений** имеют свои индивидуальные, присущие только им признаки, по которым их можно распознать и классифицировать в отдельные общие группы. При этом в качестве основного классифицирующего признака выступает метод, с помощью которого преступником осуществляется целенаправленное воздействие на средства вычислительной техники и компьютерную информацию. Выделяют следующие общие группы:

1. изъятие СВТ;
2. перехват информации;
3. несанкционированный доступ к СВТ и компьютерной информации;
4. манипуляция данными и управляющими командами;
5. комплексные методы.

К первой относятся традиционные способы совершения преступлений, в которых действия преступника направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимается любое СВТ. С уголовно-правовой точки зрения подобные преступные деяния будут квалифицироваться по совокупности соответствующими статьями УК Российской Федерации. Например, как свидетельствуют материалы одного из уголовных дел, в г. Волжском Волгоградской области преступники, перепилив с помощью ножовки по металлу прутья оконных металлических решеток, проникли в 3.00 час. в необорудованный охранной сигнализацией операционный зал Сбербанка, откуда похитили два системных блока персональных компьютеров стандартной конфигурации типа IBM PC/AT386 и PC/AT286, содержащих в своей постоянной памяти сведения на всех вкладчиков - физических и юридических лиц, кредиторов - с полными установочными данными. Такой способ совершения компьютерного преступления достаточно прост и традиционен и относится к рассматриваемой группе, как и те, которые связаны с противоправным изъятием различных физических носителей ценной информации - дискет, оптических и магнитооптических компакт-дисков, пластиковых карт, интегральных микросхем и т. п.

Ко второй группе способов совершения компьютерных преступлений относятся те, которые основаны на получении преступником компьютерной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемые в оперативно-розыскной деятельности. К ним, в частности, относятся:

1) Пассивный (бесконтактный) перехват, осуществляемый путем дистанционного перехвата электромагнитных излучений, испускаемых при работе СВТ:

- *перехват оптических сигналов (изображений)* в видимом, инфракрасном (ИК) и ультрафиолетовом (УФ) диапазонах волн (осуществляется преступником с помощью оптических, оптикоэлектронных, телевизионных, тепловизионных, лазерных, фото- и других визуальных средств съема информации);

- *перехват акустических сигналов*, распространяющихся в воздушной, водной и твердой средах (осуществляется с использованием акустических, гидроакустических, виброакустических, лазерных и сейсмических средств;

- *перехват электромагнитных сигналов*, распространяющихся по техническим каналам основных и вспомогательных средств и систем в виде паразитных информативных физических полей: побочных электромагнитных излучений и наводок (ПЭМИН), паразитных модуляций ВЧ сигналов, паразитных информативных токов и напряжений, образуемых за счет эффекта электроакустического преобразования сигналов в сетях электросвязи, электрофикации, электрочасофикации, охранно-пожарной сигнализации, в сетях СВТ, в блоках СВТ и т. п.

2) Активный (контактный) перехват, осуществляемый путем непосредственного подключения к СВТ или системе передачи данных с помощью различных штатных оперативно-технических и специально изготовленных, разработанных, приспособленных и запрограммированных средств негласного получения информации, иногда с использованием скрытых (замаскированных, зашифрованных) каналов. В данном случае преступник может целенаправленно воздействовать на СВТ в целом, его составляющие, на систему санкционирования доступа, на каналы передачи данных и на саму компьютерную информацию.

К третьей группе - относятся способы совершения компьютерного преступления, направленные на получение преступником несанкционированного доступа к СВТ, например, с использованием метода легендирования («электрик», «сантехник», «мастер по ремонту телефонов», «сотрудник рекламного агентства», «сотрудник сервисной обслуживающей организации» и т. п.), а также путем несанкционированного подключения к системе передачи компьютерной информации с целью перехвата управления вызовом абонента сети «на себя» и т. п.

Четвертая группа - это действия преступника, связанные с использованием методов манипуляции входными-выходными данными и управляющими командами средств вычислительной техники. Они используются очень часто и достаточно хорошо известны сотрудникам подразделений по борьбе с экономическими преступлениями, например, осуществление подмены входных и выходных данных бухгалтерского учета в процессе автоматизированной обработки документов или внесение умышленного изменения в существующую программу, заведомо приводящего к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. В качестве наглядных примеров можно привести такие способы, как «троянский конь», «троянская матрешка», «салями», «воздушный змей», «временная» или «логическая бомба», «люк», «компьютерный вирус» и т. п.

К пятой группе относятся комплексные способы совершения компьютерного преступления, основанные на применении преступником двух и более способов различных групп, причем один из них всегда используется как основной, а другие выполняют вспомогательные функции, например, сокрытие следов преступления.

Обобщение практики расследования компьютерных преступлений позволяет выделить следующие *основные обстоятельства, подлежащие обязательному установлению и доказыванию* по делам рассматриваемой категории:

1) Наличие преступления (либо это правонарушение иного рода); непосредственная причина (причины) нарушения безопасности компьютерной информации и орудий ее обработки; не является ли происшедшее следствием непреодолимых факторов.

2) Объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности).

3) Предмет преступного посягательства.

4) Способ совершения преступления.

1. Наименование и назначение объекта, где совершено преступление.
2. Конкретное место совершения преступления в данном предприятии, учреждении, организации, на участке местности; наличие иных мест совершения преступления (было ли преступление совершено дистанционно извне помещения - по каналам электросвязи и локальной вычислительной сети).
3. Режим работы объекта.
4. Средства вычислительной техники и компьютерной информации, с помощью которых совершено преступление (тип, вид, модификация, функциональное назначение, техническое состояние и другие характеристики). Конкретный терминал или участок сети (абонентский номер, код, шифр, рабочая частота).
5. Режим работы СВТ.
6. Возможность утечки конфиденциальной информации.
7. Период (дата, время) совершения преступления.
8. Размер материального ущерба, из чего он складывается.
9. Служебные действия и операции технологического процесса, с которыми связано преступление; перечень должностных лиц или работников, несущих ответственность и имеющих непосредственное отношение к данным действиям (операциям) в силу технологии производства или командно-административного управления.
10. Мотив совершения преступления (корысть, месть, хулиганские побуждения, демонстрация личных интеллектуальных способностей, с целью сокрытия другого преступления и др.); цели, преследуемые и достигнутые преступником; наличие у преступника в момент совершения преступления состоянии внезапно возникшего сильного душевного волнения, аффекта, либо психического заболевания (информационного невроза или компьютерной фобии).
11. Субъект преступления, его характеристика. Если преступление совершено группой лиц, анализ ее состава и роли каждого соучастника.
12. Наличие причинной связи деяний с наступившими последствиями. Необходимо проверить и доказать, что именно деяния данного лица и обязательно те, которые ему инкриминируются, являются причиной наступивших последствий, например, наличие минимально необходимых специальных познаний у преступника.
13. Причины и условия, способствовавшие подготовке, совершению и сокрытию преступления; факторы, усугубившие их проявление (нарушения нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам; не подлежат ли они привлечению к уголовной ответственности за допущенные нарушения, способствовавшие совершению расследуемого преступления, например, по ст. 274 УК РФ).

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран.

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

* + **QA - Несанкционированный доступ и перехват**
  + **QAH** - компьютерный абордаж
  + **QAI** - перехват
  + **QAT** - кража времени
  + **QAZ** - прочие виды несанкционированного доступа и перехвата
  + **QD - Изменение компьютерных данных**
  + **QUL** - логическая бомба
  + **QDT** - троянский конь
  + **QDV** - компьютерный вирус
  + **QDW** - компьютерный червь
  + **QDZ** - прочие виды изменения данных
  + **QF - Компьютерное мошенничество**
  + **QFC** - мошенничество с банкоматами
  + **QFF** - компьютерная подделка
  + **QFG** - мошенничество с игровыми автоматами
  + **QFM** - манипуляции с программами ввода-вывода
  + **QFP** - мошенничества с платежными средствами
  + **QFT** - телефонное мошенничество
  + **QFZ** - прочие компьютерные мошенничества
  + **QR - Незаконное копирование**
  + **QRG** - компьютерные игры
  + **QRS** - прочее программное обеспечение
  + **QRT** - топография полупроводниковых изделий
  + **QRZ** - прочее незаконное копирование
  + **QS - Компьютерный саботаж**
  + **QSH** - с аппаратным обеспечением
  + **QSS** - с программным обеспечением
  + **QSZ** - прочие виды саботажа
  + **QZ - Прочие компьютерные преступления**
  + **QZB** - с использованием компьютерных досок объявлений
  + **QZE** - хищение информации, составляющей коммерческую тайну
  + **QZS** - передача информации конфиденциального характера
  + **QZZ** - прочие компьютерные преступления

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

**Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:**

**QAH** - "Компьютерный абордаж" (хакинг - hacking): доступ в компьютер или сеть без нрава на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

**QAI** - перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственною подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

* + "Жучок" (bugging) - характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
  + "Откачивание данных" (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
  + "Уборка мусора" (scavening) - характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;
  + метод следования "За дураком" (piggbackiiig), характеризующий несанкционированное проникновение, как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;
  + метод "За хвост"(between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;
  + метод "Неспешного выбора" (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;
  + метод "Поиск бреши" (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
  + метод "Люк" (trapdoor), являющийся развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу;
  + метод "Маскарад" (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
  + метод "Мистификация"(spoofing), который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

**QAT** - кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

**Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:**

**QDL/QDT** - логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь - заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

**QDV** - вирус (virus): изменение компьютерных данных или программ, без права на то, путем внедрения или распространения компьютерного вируса.

Компьютерный вирус - это специально написанная программа, которая может "приписать" себя к другим программам (т.е. "заражать" их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

* + *резервирование* - копирование FAT, ежедневное ведение архивов измененных файлов - это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты;
  + *профилактика* - раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на "непотопляемые отсеки" - зоны с установленным режимом "только для чтения", хранение неиспользуемых программ в архивах, использование специальной "инкубационной" зоны для записи новых программ с дискет, систематическая проверка ВООТ-сектора используемых дискет и др.;
  + *анализ* - ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;
  + *фильтрация* - использование резидентных программ типа FluShot Plus, MaceVaccinee и других для обнаружения попыток выполнить несанкционированные действия;
  + *вакцинирование* - специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заряжения программы или всего диска;
  + *терапия* - деактивация конкретного вируса п отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага.

Понятно, что избавится от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

**QDW** - червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

**Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:**

**QFC** - компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

**QFF** - компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

**QFG** - мошенничества и хищения, связанные с игровыми автоматами.

**QFM** - манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные систе-мы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

**QFP** - компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

**QFT** - телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

**Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлении:**

**QRG/QRS** - незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

**QRT** - незаконное копирование топографии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изде-лия, произведенного с использованием данной топографии.

**Компьютерный саботаж (QS) составляют следующие виды преступлений:**

**QSH** - саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ;вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

**QSS** - компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

**К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие:**

**QZB** - использование электронных досок объявлений (BBS) для хра-нения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

**QZE** - хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;

**QZS** - использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия.

* + *"Временная бомба"* - разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;
  + *"Асинхронная атака"* (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.
  + *"Моделирование"* (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления.