Содержание:

Введение

С повышением значимости данных в абсолютно всех областях работы возрастает значимость и роль компьютерной информации как одной с наиболее известных конфигураций формирования, применения, передачи данных. А с повышением значимости компьютерной информации необходимо увеличивать степень её охраны с помощью технических, организационных и особенно законных мер.

Компьютерные правонарушения многоаспектны, и вследствие того они имеют все шансы относиться к самым различным типам противозаконных посягательств и различаться не только лишь по предмету посягательства, однако и согласно методам, аргументам и иным показателям. Одним-единственным основанием отнесения правонарушения к этой группы считается присутствие средства вычислительной техники равно как носителя охраняемой законодательством компьютерной информации, выступающего в качестве предмета либо орудия совершения правонарушения. По этой причине криминалистическая оценка компьютерных правонарушений различается конкретной особенностью.

Стержневой базой компьютерных правонарушений считаются предустановленные уголовным законодательством социально опасные действия, посягающие в безопасность компьютерной информации и орудий её обрабатывания, назначенные в специальную главу № 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации.

Под компьютерной информацией законодателем при этом подразумевается информация в машинном носителе, в ЭВМ, концепции ЭВМ либо их сети, т.е. машинная информация, циркулирующая в вычисляемой сфере, отмеченная в физиологическом носителе в фигуре, легкодоступной восприятию ЭВМ, либо переходящая согласно каналам электросвязи с помощью электромагнитных сигналов с одной ЭВМ в иную, с ЭВМ в удаленное устройство, или в управляющий датчик оборудования.

С каждым годом, по мере формирования компьютерных концепций и информативных технологий, число компьютерных правонарушений постоянно увеличивается. Согласно сведениям Основного информативного центра МВД

Российской федерации, в 2013 г. было свершено 13723 компьютерных преступлений, то что практически в 2 раза побольше согласно сопоставлению с 2003 года - 7053[1].

Все это призывает непрерывного совершенствования методов и мер предотвращения и выявления компьютерных правонарушений, и поэтому рассматриваемая в данной работе задача является очень важной.

Объект изучения: процессы предотвращения и выявления компьютерных правонарушений.

Предмет изучения: оценка преступлений в области компьютерной информации, характерные черты их профилактики, метод и стратегия изготовления единичных следственных операций при их выявлении.

Цель деятельность: предоставить характеристику правонарушениям в области компьютерной данных и обнаружить характерные черты их следствия и профилактики.

Задачи деятельность:

1. Исследовать методы совершения компьютерных правонарушений и предоставить их систематизацию.

2. Установить главные методы и мероприятия согласно предотвращению компьютерных правонарушений.

3. Обнаружить характерные черты технологии следствия правонарушений в области компьютерной данных.

3. Обнаружить характерные черты стратегии изготовления единичных следственных операций согласно правонарушениям в области компьютерной данных.

Глава 1. Способы совершения компьютерных преступлений и их предупреждение

1.1. Способы совершения компьютерных преступлений и их классификация

Главным и обусловливающим компонентом криминалистической характеристики каждого, в этом части и компьютерного, преступления представляется комплекс информации, описывающих метод его совершения.

Под методом совершения преступления как правило понимают объективно и субъективно предопределенную концепцию действия субъекта до, в момент и в последствии совершения правонарушения, оставляющего различного рода свойственные следы, позволяющие с поддержкой криминалистических способов и средств приобрести представление о сути происшедшего, своеобразии противозаконного действия правонарушителя, его единичных индивидуальных данных и соответственно установить более подходящие способы заключения проблем выявления преступления.

В.В. Крылов систематизировал способы совершения компьютерных преступлений в 5 ключевых групп. Рядом данном в свойстве главного группирующего признака представляет способ применения злоумышленником тех либо других операций, обращенных в приобретение доступа к средствам компьютерной техники. Следуя данным признаком, В.В. Крылов подчеркнул последующие единые категории:

1) выемка денег компьютерной техники (затем - СКТ);

2) перехват данных;

3) неразрешенный допуск к СКТ;

4) манипуляция сведениями и правящими командами;

5) комплексные способы[2].

К первой команде принадлежат классические методы совершения обыкновенных типов («некомпьютерных») правонарушений, в каковых воздействия правонарушителя ориентированы выемка постороннего имущества. Отличительной характерной Особенностью предоставленной категории методов совершения компьютерных правонарушений будет этот случай, что в них средства компьютерной техники станут постоянно представлять только лишь в свойстве объекта преступного посягательства. К примеру, прокуратурой г. Кургана в 2013 г.

расследовалось уголовное дело согласно прецеденту убийства частного бизнесмена. В процессе обыска в жилплощади мертвого следователем был изъязвят личный компьютер. Согласно существующей своевременной информации в памяти данной ЭВМ убитый имел возможность сохранять фамилии, адреса собственных заимодавцев и должников. В будущем данный компьютер согласно заключению следователя был вручен в 1 из компьютерных компаний с целью производства исследования содержимого его дисков памяти. В ту же ночь с здания данной компьютерной компании посредством отгиба решеток была произведена кража этого ПК. В следствии этого, что изъятие и передача ЭВМ были сделаны следователем с рядом процессуальных нарушений, это преступление осталось никак не открытым[3].

К второй команде принадлежат методы совершения компьютерных правонарушений, базирующиеся в поступках правонарушителя, обращенных в приобретение информации и машинной информации с помощью употребления способов аудиовизуального и электромагнитного перехвата, хорошо промышляемых в эффективно-розыскной работы правоохранительных органов.

Непосредственный динамичный перехват исполняется с поддержкой включения к телекоммуникационному оборудованию ПК, к примеру направления принтера либо телефонному проводу канала взаимосвязи, или напрямую через соответственный порт личного ПК.

Электромагнитный (пассивный) перехват базируется в регистрации электромагнитных излучений, появляющихся рядом функционировании многочисленных денег компьютерной техники, в том числе и ресурсы коммуникации. Волны, излучаемые электронно-светолучевой трубкой монитора, обдающие в себя определенную информацию с помощью специализированных устройств можно получать в дистанции вплоть до 1000 м.

Аудиоперехват либо устранение данных согласно виброакустическому каналу представляется более опасным и довольно популярным. Данный метод съема данных обладает 2 разновидности. 1-ая состоит в аппарате подслушивающего устройства в аппаратуру средств обрабатывания данных. 2-ая - в аппарате спецмикрофона в инженерно-промышленные установки за границами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видео перехват состоит в поступках правонарушителя, обращенных в получение информации посредством применения разной видеооптической техники.

«Уборка мусора» предполагает собою незаконное применение преступником научно-технических остатков информативного движения, отметенных пользователем в последствии работы с компьютерной техникой. К примеру, в том числе и удаленная из памяти компьютера информация, подлежит стремительному возобновлению и неразрешенному изъятию с поддержкой специализированных программных денег[4].

К третьей команде методов совершения компьютерных правонарушений принадлежат воздействия правонарушителя, нацеленные на приобретение неразрешенного допуска к медикаментам компьютерной техники. К ним причисляются следующие:

1. «За дураком». Данный метод применяется злоумышленником посредством включения компьютерного терминала к каналу взаимосвязи через коммуникационную технику в тот период времени, когда работник, отвечающий за работу средства компьютерной техники, кратковременно оставляет свое рабочее место, бросая терминал в интенсивном порядке.

2. «За хвост». При данном методе съема данных злоумышленник подключается к линии взаимосвязи легитимного юзера и ждет сигнала, помечающего исход работы, перехватывает его в себя и реализовывает допуск к организации.

3. «Компьютерный абордаж», согласно сути возникающий предварительной стадией компьютерного правонарушения. Этот метод совершения компьютерного правонарушения осуществляется злоумышленником посредством неожиданного перебора клиентского номера компьютерной организации с применением модемного устройства. Порой с целью данных целей применяется намеренно основанная самодельная, или фабричная схема автоматического отыскивания пароля. Метод ее работы состоит в том, чтобы, применяя быстродействие нынешних компьютерных устройств, перебирать всегда вероятные виды комбинаций букв, чисел и особых знаков, и в случае совпадения композиции знаков делать автоматическое объединение отмеченных абонентов.

В последнее время правонарушителями начал динамично применяться способ «интеллектуального перебора», базирующийся в выборе предвидимого пароля, отталкиваясь с предварительно установленных предметных компаний его приспособления. В данном случае программе - «взломщику» переходят определенные начальные сведения о личности автора пароля. Согласно анализам экспертов, это дает возможность наиболее чем в 10 порядков уменьшить число

вероятных альтернатив перебора символов и в столько же - время в отбор пароля.

4. «Неспешный выбор». При этом методе совершения правонарушения, злоумышленник реализовывает неразрешенный допуск к компьютерной организации посредством пребывания слабых областей в ее охране. Данный метод Весьма популярен из числа так называемых взломщиков. В Сети интернет и прочих массовых компьютерных сетях подходит непрерывный отбор, обмен, приобретение и реализация развороченных взломщиками проектов. Имеются специализированные телеконференции, в каковых протекает рассмотрение взламывающих проектов, вирусов, проблем их формирования и распространения.

5. «Брешь». В отличие с «неспешного выбора», если выполняется отбор уязвимых областей в охране компьютерной организации, при данном способе злоумышленником исполняется их детализация: формируются области, имеющие ошибку либо незадачливую логику программного строения. Обнаруженные подобным способом «бреши» имеют все шансы применяться злоумышленником неоднократно, пока никак не станут выявлены.

6. «Люк». Этот метод представляется закономерным продолжением предыдущего. В данном случае в обнаруженной «бреши» схема «разрывается» и туда в дополнение злоумышленник внедряет 1 либо ряд команд. Такого рода «люк» «открывается» согласно потребности, а включенные команды автоматом исполняются. Нужно отметить, что же такой «черный вход» в якобы защищенную концепцию имеется в любой сертифицированной государством программе, однако об этом никак не принято распространяться вслух[5].

К четвертой группе методов совершения компьютерных правонарушений принадлежат воздействия правонарушителей, сопряженные с применением способов манипуляции сведениями и управляющими командами денег компьютерной техники. Данные способы более часто применяются правонарушителями с целью совершения разного рода беззаконных действий и довольно отлично известны работникам подразделений правоохранительных органов, которые специализируются по борьбе с экономическими правонарушениями. Более хорошо применяются последующие методы совершения компьютерных правонарушений, имеющих отношение к данной команде.

1. «Подмена данных» - более легкий и в следствии этого весьма Нередко используемый метод совершения правонарушения. Воздействия правонарушителей в данном случае ориентированы в изменение либо внедрение новых данных,

которые исполняются, как правило, рядом вводе-выводе данных.

2. «Троянский конь». Этот метод состоит в сокровенном внедрении в чужое программное обеспечение намеренно разработанных проектов, которые, попадая в справочно-вычисляемые организации, принимаются исполнять новые, никак не планировавшиеся законным собственником проекта, с одновременным сохранением прежней ее работоспособности. В согласовании с ст. 273 Уголовного кодекса РФ подтакого рода проектом понимается «программа для ЭВМ, приводящая к неразрешенному уничтожению, блокированию, модификации или копированию данных, нарушению деятельность ЭВМ, системы ЭВМ или их сети»[6].

По существу, «троянский конь» - это совершенствование ранее рассмотренного нами метода «люк» с той лишь разницей, что он «открывается» никак не при поддержки прямых операций самого правонарушителя («вручную»), а автоматом - с применением специально приготовленной для этих целей проекта без последующего непосредственного участия самого правонарушителя.

С поддержкой этого метода злоумышленники как правило отчисляют в предварительно доступный расчет установленную необходимую сумму с каждой операции. Вероятен тут и вид повышения правонарушителями лишних сумм в счетах при машинальном пересчете рублевых остатков, сопряженных с переходом к коммерческому курсу соответствующей денежной единицы.

Разновидностями подобного метода совершения компьютерных правонарушений представляется введение в программы «логических» и «временных бомб», всевозможных компьютерных вирусов. С уголовно-правовой точки зрения, в соответствии с ст. 273 Уголовного кодекса РФ, перед компьютерным вирусом необходимо понимать вредоносную программу для ЭВМ, способную самостоятельно примыкать к иным программ («заражать» их) и при запуске последних выполнять разные ненужные действия: порчу файлов, изменение, стирание информации и данных, захлестывание машинной памяти и формирование препятствий в службе ЭВМ.

3. Подражание (размножение) проектов с преодолением программных денег охраны. Данный метод учитывает противозаконное формирование копии основной дискеты, трансформацию кодировки организации охраны, прогнозирование призыва к основной дискете, устранение организации охраны с памяти ПЭВМ и т.п. [7]

Не тайна, что сдерживающая часть программного обеспеченья, применяемого в Рф, представляется пиратскими копиями взломанных хакерами программ. Наиболее известной операторной концепцией в Рф представляется MicrosoftWindows. Согласно статистике, в часть данной платформы требуется больше 7% процентов российского рынка операторных систем. Собственным несомненным триумфом в российском рынке Windowsобязана деятельности компьютерных пиратов. Согласно сведениям антипиратской организации BSA, больше 90% применяемых в Рф проектов введены в ПК без лицензий, в то время равно как в США никак не наиболее 24%.

Можно привести в качестве образца и хорошо знакомую российскую СПС «Консультант Плюс» содержащую время от времени обновляемую компьютерную основу отечественного законодательства. Невзирая в стабильную службу разработчиков программного обеспечения компании согласно улучшению конструкций защиты, тыс. незаконных копий взломанной программы обладают хождение в территории страны.

Успехи взломщиков до такой степени велики, что же, к примеру, США решили использовать их в информативной борьбе. С времени официального признания в 1993 г. военно-политическим руководством США «информационной войны» в свойстве одной с составляющих государственной боевой стратегии, ускоренными темпами проходят розыски способов, конфигураций и денег ее ведения. Так, в последние года всегда чаще рассказывают о необходимости привлечения взломщиков в разных стадиях «информационной войны».

Хакеры более продуктивно могут быть применены в рубеже сбора разведывательной информации и данных о компьютерных сетях и режимах возможного противника. Они ранее скопили полный навык в угадывании и выявлении паролей, применении болезненных областей в режимах защиты, обмане легитимных пользователей и вводе вирусов, «троянских коней» и т.п. в программное обеспечение ПК. Искусство проникновения в компьютерные сети и организации под видом легитимных пользователей предоставляет взломщикам вероятность стирать все следы собственной работы, что же обладает огромное значимость с целью эффективной шпионской работы. Помимо этого, помеченная видимость легитимного пользователя предоставляет вероятность хакеру-шпиону создать ошибочную концепцию и внедрить нее в сеть противника в качестве легитимного пользователя информации.

1.2. Предупреждение компьютерных преступлений

Мировой опыт борьбы с преступностью говорит о том, что один из первенствующих течений решения проблемы успешного противодействия современной преступной деятельности представляется интенсивное применение правоохранительными органами всевозможных мер профилактического характера.

Большинство иностранных экспертов прямо указывает в то, что предостеречь компьютерное преступление постоянно значительно проще и легче, Нежели его выявить и выяснять.

Обычно акцентируют 3 главные категории граней предотвращения компьютерных правонарушений, образующих в собственной совокупности целую концепцию войн с данным общественно небезопасным феноменом, а в частности:

1) правовые;

2) организационно-технические;

3) криминалистические.

К правовым мерам предотвращения компьютерных правонарушений в первую очередность принадлежат нормы законодательства РФ, устанавливающие уголовную ответственность за указанные выше незаконные действия. Данные нормы:

- предоставляют адвокатское определение основных частей информативной технологии равно как предметов законный защиты;

- определяют и фиксируют полномочия и прямые обязанности владельца в эти объекты;

- устанавливают законный порядок функционирования денег информативных технологий;

- устанавливают группы допуска установленных субъектов к определенным типам данных;

- определяют группы секретности информации и данных;

- предоставляют установление и пределы законного использования термина «конфиденциальная информация», а кроме того возлагают прямые обязанности наопределенных субъектов согласно ее защите с различных факторов[8].

Организационно-технические мероприятия предотвращения компьютерных правонарушений исполняется согласно следующим тенденциям:

1) соотношение административных операций условиям компьютерной защищенности;

2) создание проблем промышленной охраны компьютерных улов и компьютерного оборудования;

3) создание стереотипов обрабатывания информации и стереотипов компьютерной защищенности;

4) выполнение профессиональной политики с целью обеспеченья компьютерной защищенности.

Необходимо создавать базисные условия безопасности, предъявляемые к компьютерным сетям. В их числе:

- пригодность - гарантия того, что сеть пригодна с целью обеспеченья организованного допуска;

- регулируемая общедоступность - гарантия, что сеть гарантирует допуск только лишь санкционированному пользователю с целью решения организованных проблем;

- неприкасаемость - охрана информации с несанкционированного их изменения и ликвидирования;

- секретность - охрана информации с неразрешенного выявления;

- защищенность передачи информации - гарантия того, что идентификация пользователей, качество передаваемых данных, время и продолжительность передачи информации гарантированы.

На базе данных условий обязаны формироваться надлежащие механизмы технологического контролирования, отвечающие последующим аспектам:

1) целостность - базовая надежность, гарантирующая, что система функционирует равно как следует;

2) вероятность контроля - умение писать информацию, что может обладать значимость в выявлении и изучении усилий посягательства в ресурсы компьютерной техники и прочих событий, имеющих отношение к проблемам защищенности системы.

В следствии практической осуществлении данных граней будет возможно:

- регулировать физический допуск к средствам компьютерной техники (СКТ);

- регулировать электромагнитное излучение аппаратных СКТ;[9].

Таким образомцели и основные положения защиты информации предполагают:

а) предотвращение утечки, хищения, утраты, искажения и подделки информации;

б) предотвращение угроз безопасности личности, общества и государства;

в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

г) обеспечение правового режима функционирования документированной информации как объекта собственности;

д) сохранение государственной тайны и конфиденциальности документированной информации;

е) обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

По методам применения тех или иных организационно-технических мер предупреждения компьютерных преступлений специалистами отдельно выделяются три их основные группы:

1) организационные;

2) технические;

3) комплексные (сочетающие в себе отдельные методы двух первых групп)[10].

Организационные мероприятия защиты СКТ включают в себе комплекс организационных событий согласно выбору, контролю и инструктажу персонала, участвующего в абсолютно всех стадиях информативного процесса; разработке проекта восстановления информационных предметов в последствии выхода их с строя; организации программно-технического сервиса СКТ; возложению дисциплинарной ответственности на лиц по обеспечению защищенности определенных СКТ; исполнению режима секретности при функционировании компьютерных конструкций; обеспечиванию режима физиологической защиты объектов; материально-техническомуобеспечиванию и т.д. и т.п. Организационные события, согласно взгляду многочисленных экспертов, занимающихся проблемами защищенности компьютерных конструкций, представлены важным и одним из эффективных средств защиты данных, в то же время являясь фундаментом, в каком основывается в будущем вся концепция защиты.

Анализ веществ российских уголовных дел дает возможность совершить заключение о этом, что же главными факторами и критериями, содействующими совершению компьютерных правонарушений, в основной массе случаев стали:

1) неконтролируемый доступ работников к пульту управления (клавиатуре) ПК, применяемого равно как независимо, так и в свойстве рабочей станции автоматизированной узы с целью дистанционной передачи информации основных бухгалтерских бумаг в ходе исполнения экономических действий;

2) бесконтрольность за поступками обслуживающего персонала, что же дает возможность злоумышленнику беспрепятственно пользоваться ЭВМ в качестве орудия совершения правонарушения;

3) низкий уровень программного обеспеченья, что никак не обладает контрольной защиты, обеспечивающей контроль соотношения и точности вводимой информации;

4) недоработка парольной организации охраны с неразрешенного допуска к рабочей станции и ее программномуобеспечиванию, что никак не гарантирует правдивую идентификацию пользователя согласно личным биометрическим характеристикам;

5) недостаток должностного лица, отвечающего за порядок секретности и конфиденциальности коммерческой информации и ее защищенности в части

охраны денег компьютерной техники с неразрешенного допуска;

6) недостаток категоричности допуска работников к документации жесткой экономической отчетности, в т. ч. пребывающей в форме машинной информации;

7) недостаток соглашений (договоров) с работниками на предмет неразглашения торговой и должностной тайны, индивидуальных данных и другой секретной информации[11].

Применяемые в большинстве организаций системы позволяют обычно использование таких мер безопасности, как пароли, недоступность программных и информационных файлов, а также другие меры, которые почти не практикуются, либо используются в ограниченном масштабе. Причины этого различные. Одна из основных - финансовая, поскольку, внедрение защитной системы является делом дорогостоящим. Кроме того, в целях экономии на одном и том же компьютере нередко совершаются многопрофильные операции, что в свою очередь повышает риск несанкционированного доступа. Контроль и проверки правильности использования компьютеров также требуют дополнительных финансовых затрат, и если в течение нескольких лет не происходит никаких инцидентов, то контроль либо ослабевает, либо не осуществляется вообще. В то же время для эффективной безопасности от компьютерных преступлений всего лишь необходимо:

1) просмотреть всю документацию в учреждении, организации;

2) ознакомиться с функциями и степенью ответственности каждого сотрудника;

3) определить возможные каналы утечки информации;

4) ликвидировать обнаруженные слабые звенья в защите[12].

Таким способом более эффективным направлением в предупреждении незаконных посягательств представляется единое применение разных мер предотвращения компьютеерных правонарушений: координационных, аппаратных и программных. К примеру, с целью снижения угрозы вирусных посягательств в СКТ, согласно взгляду экспертов, нужно начать последующие единые координационно-промышленные мероприятия, какие имеют все шансы быть сокращены либо расширены согласно собственному содержанию, отталкиваясь с любой конкретной ситуации. С целью этого нужно:

1. Оповещать абсолютно всех работников института, учреждения, использующих СКТ, об опасности и вероятном ущербе в случае совершения вирусного

посягательства.

2. Никак не осуществлять неофициальные взаимосвязи с иными организациями, связанные с обменом программных денег. Запрещать работникам давать в рабочее место программные средства (ПС) “со стороны” с целью работы с ними в СКТ, пребывающих в учреждении, организации согласно пункту работы сотрудника. В последнем случае для этих целей может быть создано особое самостоятельное рабочее место с целью испытания подобных ПС на предмет определения присутствия либо отсутствия вих средств вирусного характера. Должны использоваться только лишь официально распространяемые ПС, хранящиеся в аттестированных и опломбированных носителях механической данных.

3. Запрещать работникам пользоваться и сохранять в носителях и в памяти ПЭВМ компьютерные игры, представляющие источником высокой угрозы с целью защищенности компьютерных систем. В случае если подобное запрещение никак не может быть гарантированно; в таком случае реализовать особое игровое место либо всеобщий видеоигровой файл, всегда управляемый работниками работы компьютерной безопасности и содержащий «иммунные» ресурсы противовирусной охраны.

4. Оповестить работников учреждения с применения ПС и носите-лей машинной информации, обладающих возникновение с учебных учреждений разного уровня и профиля.

5. В случае если в ходе работы появится потребность в применении сто-ронних информативных компьютерных сеток, в таком случае для этих целей нужно в неукоснительном режиме особо отметить особое стендовое оснащение с неизбежной его обособленностью с прочих СКТ. Всегда комп.данные, прибывающие с наружной компьютерной узы, обязаны непременно контролироваться (тестироваться).

6. Реализовать архив снимок ПС, применяемых в прямой службе учреждения с синхронным изъятием неразрешенного допуска к данному архиву.

7. Регулировать управление журналов операторов ЭВМ (деятельность ЭВМ). В случае отсутствия надлежащей записи при наличии трудящегося работника получать дисциплинарные меры влияния.

8. Определить организации охраны данных в особенно значимых ЭВМ. Заактивировать в их специальные комплексные противовирусные программные

ресурсы в неукоснительном режиме.

9. Всегда регулировать выполнение определенных законов обеспеченья защищенности СКТ и использовать мероприятия дисциплинарного влияния к лицам, сознательно или неоднократно нарушавшим их.

Глава 2. Методика и тактика расследования преступлений в сфере

компьютерной информации

2.1. Особенности методики расследования преступлений в сфере компьютерной информации

Общеизвестно, собственно одними мерами предотвращения порой получается избежать беззаконное посягательство. В этой связи встает необходимость заниматься не совсем только вопросами обороны средств компьютерной техники, ведь и улаживать вопросы расследования компьютерных правонарушений.

В Экспертно-криминалистическом центре МВД прошел классификационный тест лиц, замешанных в использовании компов для совершения противоправных действий. Обобщенный портрет российского злонамеренного взломщика, сделанный на базе уголовного преследования этого семейства персон, смотрится приблизительно так: данное представитель сильного пола в возрасте от 15 до 45 лет, либо имеющий большой опыт на компе, или практически не обладающий этим навыком; в минувшем к уголовной ответственности не привлекался; считается ясной, думающей персоной, способной брать на себя сознательные решения; превосходный, честный сотрудник, по нраву нетерпимый к шуткам и к утрате собственного общественного статуса в масштабах категории находящихся вокруг его жителей нашей планеты; предпочитает уединенную работу; прибывает на службу первым и уходит заключительным; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы[13].

По сведениям того же Экспертно-криминалистического центра МВД, принципиальная схема организации взлома защитных механизмов информационных системы достаточно однотипна. Профессиональные компьютерные взломщики обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо, подкупают сотрудников организации, знакомых с деталями электронных платежей

и паролями, и работников телефонной станции, чтобы обезопаситься на случай поступления запроса от служб безопасности. Нанимают охрану из бывших сотрудников МВД. Чаще всего взлом компьютерной сети осуществляется рано утром, когда дежурный службы безопасности теряет свою бдительность, а вызов помощи затруднен.

Ниже представлена общая схема расследования неправомерного доступа к компьютерной информации. В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

1. Установление факта неправомерного доступа к информации в компьютерной системе или сети.

2. Установление места несанкционированного проникновения в компьютерную систему или сеть.

3. Установление времени совершения преступления.

4. Установление надежности средств защиты компьютерной информации.

5. Установление способа несанкционированного доступа.

6. Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления.

7. Установление вредных последствий преступления.

8. Выявление обстоятельств, способствовавших преступлению[14].

На признаки несанкционированного доступа или подготовки к нему могут указывать следующие обстоятельства: появление в компьютере фальшивых данных; не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств; частые сбои в процессе работы компьютеров; участившиеся жалобы клиентов компьютерной системы или сети; осуществление сверхурочных работ без видимых на то причин; немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков; неожиданное приобретение сотрудником домашнего дорогостоящего компьютера; чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительным предлогом перезаписи программ для компьютерных игр; участившиеся случаи перезаписи отдельных данных без серьезных на то причин; чрезмерный интерес отдельных

сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

Определить место и время непосредственного применения технических средств удаленного несанкционированного доступа (не входящих в данную компьютерную систему или сеть) на практике бывает достаточно трудно. Для установления этих данных необходимо привлекать специалистов.

Несанкционированный доступ к закрытой компьютерной системе или сети является технологически весьма сложным действием. Совершить такую акцию могут только специалисты, имеющие достаточно высокую квалификацию. Поэтому поиск подозреваемых следует начинать с технического персонала пострадавших компьютерных систем или сетей (разработчиков соответствующих систем, их руководителей, операторов, программистов, инженеров связи, специалистов по защите информации и других)[15].

Следственная практика показывает, что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен.

При расследовании преступления, предусматривающего создание, использование и распространение вредоносных программ для ЭВМ представляется наиболее целесообразной следующая последовательность решения основных задач:

1) Установление факта и способа создания вредоносной программы для ЭВМ.

2) Установление факта использования и распространения вредоносной программы.

3) Установление лиц, виновных в создании, использовании и распространении вредоносных программ для ЭВМ.

4) Установление вреда, причиненного данным преступлением.

5) Установление обстоятельств, способствовавших совершению расследуемого преступления[16].

При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, необходимо прежде всего доказать факт нарушения определенных правил, повлекший уничтожение, блокирование или модификацию охраняемой законом компьютерной информации и причинивший существенный вред. Кроме того,

необходимо установить и доказать:

1) место и время (период времени) нарушения правил эксплуатации ЭВМ;

2) характер компьютерной информации, подвергшейся уничтожению, блокированию или модификации вследствие нарушения правил эксплуатации компьютерной системы или сети;

3) способ и механизм нарушения правил;

4) характер и размер ущерба, причиненного преступлением;

5) факт нарушения правил определенны лицом;

6) виновность лица, допустившего преступное нарушение правил эксплуатации ЭВМ;

7) обстоятельства, способствовавшие совершению расследуемого преступления.

Если следователь располагает информацией, что на объекте обыска находятся средства компьютерной техники, расшифровка данных, с которых может дать доказательства по делу, он должен заранее подготовиться к их изъятию. Необходимо обеспечить участие в ходе обыска специалиста по компьютерной технике. По прибытии на место обыска следует сразу же принять меры к обеспечению сохранности ЭВМ и имеющихся на них данных и ценной информации.

Для этого необходимо:

1) не разрешать, кому бы то ни было из лиц, работающих на объекте обыска или находящихся здесь по другим причинам (персоналу), прикасаться к ЭВМ с любой целью;

2) не разрешать, кому бы то ни было из персонала выключать электроснабжение объекта;

3) в случае если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети всю компьютерную технику, находящуюся на объекте;

4) самому не производить никаких манипуляций со средствами компьютерной техники, если результат этих манипуляций заранее неизвестен.

После принятия указанных выше неотложных мер можно приступать к непосредственному обыску помещения и изъятию средств компьютерной техники [17].

При этом следует принять во внимание следующие неблагоприятные факторы:

- возможные попытки со стороны персонала повредить ЭВМ с целью уничтожения информации и ценных данных;

- возможное наличие на компьютерах специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

- возможное наличие на ЭВМ иных средств защиты от несанкционированного доступа;

- постоянное совершенствование компьютерной техники, следствием чего может быть наличие на объекте программно-технических средств, незнакомых следователю[18].

В целях недопущения вредных последствий перечисленных факторов следователь может придерживаться следующих рекомендаций:

1. Перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера - путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель - приводит к потере информации в оперативной памяти и даже к стиранию информационных ресурсов на данном компьютере).

2. При наличии средств защиты, ЭВМ от несанкционированного доступа принять меры к установлению ключей доступа (паролей, алгоритмов и т.д.).

3. Корректно выключить питание всех ЭВМ, находящихся на объекте (в помещении).

4. Не пытаться на месте просматривать информацию, содержащуюся в компьютерах.

5. В затруднительных случаях не обращаться за консультацией (помощью) к персоналу, а вызывать специалиста, не заинтересованного в исходе дела.

6. Следует изъять все ЭВМ, обнаруженные на объекте.

7. При обыске не подносить ближе, чем на 1 м к компьютерной технике металлоискатели и другие источники магнитного поля, в т. ч. сильные осветительные приборы и некоторуюспецаппаратуру.

8. Поскольку многие, особенно неквалифицированные, пользователи записывают процедуру входа-выхода, работы с компьютерной системой, а также пароли доступа на отдельных бумажных листках, следует изъять также все записи, относящиеся к работе с ЭВМ.

9. Так как многие коммерческие и государственные структуры прибегают к услугам нештатных и временно работающих специалистов по обслуживанию средств компьютерной техники, следует записать паспортные данные у всех лиц, находящихся на объекте, независимо от их объяснений цели пребывания на объекте.

При изъятии средств компьютерной техники необходимо обеспечить строгое соблюдение требований действующего уголовно-процессуального законодательства. Для этого необходимо акцентировать внимание понятых на всех производимых действиях и их результатах, давая им при необходимости пояснения, поскольку многим участникам следственного действия могут быть непонятны производимые манипуляции. Кроме того, следует опечатывать ЭВМ так, чтобы исключить возможность работы с ними, разукомплектовки и физического повреждения основных рабочих компонентов в отсутствие владельца или эксперта. При опечатывании компьютерных устройств следует наложить один лист бумаги на разъем электропитания, расположенный на задней панели, второй - на переднюю панель вверху с захлестом на верхнюю панель и закрепить их края густым клеем. На листах бумаги должны быть подписи следователя, понятых и представителя персонала. При изъятии магнитного носителя машинной информации нужно помнить, что они должны перемещаться в пространстве и храниться только в специальных опломбированных и экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей и «наводок», направленных излучений[19].

В случае, когда необходимо сослаться непосредственно на определенный физический носитель, следует указать в протоколе его серийный (заводской) номер, тип, название (если есть) или провести его точное описание (размеры, цвет, класс, надписи, физические повреждения). При отсутствии четких внешних признаков физический носитель запечатывается в отдельную коробку (ящик, конверт) о чем обязательно делается отметка в протоколе проведения следственного действия.В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети) в обязательном порядке после его осмотра необходимо блокировать не только соответствующее помещение, но и отключать источники энергопитания аппаратуры или, в крайнем случае, создать условия лишь для приема информации с одновременным опломбированием всех необходимых узлов, деталей, частей и механизмов компьютерной системы.Если же возникла необходимость изъятия информации из оперативной памяти компьютера (непосредственно из оперативного запоминающего устройства - ОЗУ), то сделать это возможно только путем копирования соответству-ющей машинной информации на физический носитель с использованием стандартных паспортизированных программных средств с соответствующим документальным приложением и в порядке, установленном государственными стандартами[20].

2.2. Особенности тактики расследования компьютерных преступлений

Перечень неотложных следственных действий и оперативных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование. Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного работника.

Поводами и причинами для возбуждения уголовных дел в первую очередь служат: заявления граждан (конкретных потерпевших); сообщения глав компаний, учреждений, организаций и должностных лиц (основанные, обычно, на материалах контрольно - ревизионных проверок и известиях служб сохранности); сведения, приобретенные в следствии проведения оперативно -розыскных мероприятий;

непосредственное обнаружение следователем, прокурором или же судом признаков преступления; заметки, статьи и письма, опубликованные в средствах массовой информации, а также в сети «Интернет»[21].

К типичным признакам подготовки, совершения и сокрытия преступления в сфере компьютерной информации относятся:

- появление в ЭВМ, системе ЭВМ или их сети фальшивых данных; несанкционированные изменения структуры файловой системы, программного обеспечения и конфигурации ЭВМ, системы ЭВМ или их сети;

- необычные (нестандартные) проявления в работе СВТ и их программного обеспечения;

- частые сбои в работе аппаратуры;

- жалобы клиентов на предоставление некачественного доступа к ЭВМ, системе ЭВМ, их сети или компьютерной информации;

- сверхурочная работа некоторых сотрудников на ЭВМ, в системе ЭВМ или их сети, нарушение установленного графика их эксплуатации; нерегламентированный доступ к ЭВМ, системе ЭВМ, их сети и к компьютерной информации отдельных субъектов;

- нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней;

- чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию чужих распечаток (листингов) и компьютерной информации определенной категории;

- случаи перезаписи отдельных данных и компьютерной информации без серьезных требуемых на то причин; применение на рабочем месте и вынос с работы личных машинных носителей информации под различными предлогами (записи игр и т.п.);

- исследование мусорных корзин (контейнеров) с технологическими отходами компьютерной обработки информации;

- случаи утечки конфиденциальной информации, либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ЭВМ, системой ЭВМ, их сетью или компьютерной

информацией;

- создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом;

- несоответствие данных, содержащихся в первичных (исходных) документах, данным машинограмм и иным более поздним по времени создания документам;

- подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории[22].

Для преступлений в сфере компьютерной информации типичны три ситуации первоначального этапа расследования:

1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствуют.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируют и осуществляют следующие неотложные следственные действия, оперативно - розыскные, организационные и иные мероприятия:

1) получение объяснения (допрос) заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей (очевидцев);

2) вызов и инструктаж необходимых специалистов для участия в осмотре места происшествия;

3) осмотр места происшествия (с осмотром, предварительным исследованием и изъятием машинных носителей и компьютерной информации, СВТ, документов и т. п.);

4) проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, определения рабочего места преступника, обнаружения следов и других вещественных доказательств;

5) изучение справочной литературы, ведомственных нормативных актов, положений, инструкций, правил эксплуатации конкретного СВТ и порядка работы с компьютерной информацией, а также консультации с соответствующими специалистами;

6) наведение справок в контролирующих, инспектирующих и лицензирующих организациях и их структурных подразделениях (Гостехкомиссии, налоговой инспекции, Комитете по контролю за использованием радиочастот, Энергонадзоре, Госпожнадзоре, КРУ, торговой инспекции и т.п.);

7) истребование материалов контрольных проверок, инвентаризаций и ревизий (соблюдения правил обработки информации, системы защиты конфиденциальной информации, оборота электронных документов и др.) за интересующий следствие период, в случае необходимости - организовать их производство (в т.ч. повторно);

8) выемку и последующий осмотр недостающих документов (в том числе находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия, а также орудий (СВТ, программ для ЭВМ, компьютерной информации, предметов, материалов и др.), с помощью которых они, возможно, были изготовлены;

9) допросы подозреваемых и/или свидетелей, ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации;

10) обыски на рабочих местах и по месту проживания подозреваемых;

11) назначение экспертиз - программно-технической, радиотехнической, технической, бухгалтерской, полимерных материалов и изделий из них и иных.

Дальнейшие действия планируются с учетом дополнительной информации, полученной при производстве вышеуказанных действий[23].

При наличии третьей следственной ситуации необходимо:

1) изучить поступившие материалы с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка их передачи в органы предварительного следствия. При необходимости - принять меры к получению недостающей процессуальной информации;
2) решить вопрос о возможности задержания преступника с поличным и о

необходимых в связи с этим мероприятиях;

3) личный обыск задержанного;

4) осмотр места происшествия с участием соответствующих заранее приглашенных специалистов;

4) допрос задержанного;

5) обыски на рабочем месте и по месту проживания задержанного;

6) установление связей задержанного и лиц, причастных к совершению преступления;

7) допрос свидетелей (очевидцев);

8) допрос подозреваемого;

9) выемка и осмотр следующих вещественных доказательств и документов: подлинных документов, удостоверяющих личность преступника и наличие у него соответствующих специальных познаний, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в том числе документов, находящихся в электронной форме на машинных носителях информации); орудий подготовки, совершения и сокрытия преступления; предмета преступления;

10) допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за конкретный участок работы по фактам установленных нарушений;

11) истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении с конфиденциальной информацией, с бланками строгой отчетности, компьютерной информацией, ЭВМ, системой ЭВМ, их сетью и т. п.;

12) допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с преступником;

13) анализ полученной информации и решение вопроса о необходимости назначения судебных экспертиз, проведения ревизии, инвентаризации или контрольной проверки (в том числе повторной).

В очередность перечисленных следственных действий, оперативных и организационных мероприятий могут быть внесены коррективы в зависимости от изменения ситуации[24].

Все следственные действия по делам о преступлениях в сфере компьютерной информации проводятся в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом следующих основных особенностей:

- следственное действие должно быть заблаговременно подготовлено и детально спланировано;

- в каждом следственном действии должны принимать участие специалисты четко представляющие свои задачи, права и обязанности;

- понятые должны обладать минимально необходимыми специальными познаниями в области обработки компьютерной информации (на уровне бытовых пользователей ПЭВМ), следователь и специалисты - познаниями в части полной сохранности (неизменяемости) компьютерной информации, содержащейся на осматриваемом (изымаемом) средстве электронно-вычислительной техники;

- для осмотра, обыска и выемки компьютерной информации и ее носителей заранее должны быть подготовлены необходимые СВТ и материалы[25].

При осмотре места происшествия в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации, помимо следователя, должны входить:

- специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории;

- специалист по СВТ;

- сотрудник Гостехкомиссии России, Центра защиты информации (при наличии на месте происшествия конфиденциальной компьютерной информации, машинных носителей с ней, специальных средств защиты от НСД и(или) СТС негласного получения (уничтожения, блокирования) компьютерной информации);

- специалист по сетевым технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети);

- специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи);

- оперативные сотрудники (отдела «К» или ОБЭП); участковый оперуполномоченный, обслуживающий данную территорию;

- инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, одновременно является охраняемым объектом);

- специалист для проведения цветной фото- или видеосъемки следственного действия.[26].

Если при проведении осмотра места происшествия используются СВТ и специальные поисковые технические устройства (материалы), об этом делается соответствующая отметка в протоколе следственного действия с указанием их индивидуальных признаков (тип, марка, название, заводской номер и т.д.). Кроме того, в обязательном порядке делается отметка о том, что данные СВТ перед началом следственного действия в присутствии понятых были тестированы специальным программным средством (указывают его тип, вид, название, версию, автора и другие реквизиты) на предмет отсутствия в них вредоносных программно - аппаратных средств и закладок.

Осмотр средства электронно-вычислительной техники в большинстве случаев является первоначальным следственным действием и проводится для обнаружения следов преступления; для решения вопросов о том, кем, с какой целью и при каких обстоятельствах было совершено преступление; выяснения обстановки происшедшего события; восстановления механизма совершения преступления. Проводить осмотр следует с участием специалиста[27].

Прежде всего, нужно уяснить смысл и назначение СВТ; установить, включено оно или нет; проверить его работоспособность и наличие в его памяти компьютерной информации; установить наличие или отсутствие сопряжения с каналом электросвязи и другими техническими устройствами. После этого необходимо перейти к поиску материальных следов, содержащихся на его корпусе, отдельных деталях и проводных соединениях, в его постоянной и оперативной памяти (в виде компьютерной информации).

При осмотре СВТ непозволительно применение: магнитосодержащих веществ и приборов; промышленных девайсов, производящих и излучающих электромагнитные поля и наводки (магнитный спецпорошок и кисточка, магнит,

металлоискатель, сильные осветительные оборудование, УФ и ИК излучатели и т.п.); кислотно-щелочных веществ и разогревательных устройств в избежании уничтожения (повреждения) СВТ и компьютерной данных, следов правонарушителя и правонарушения. Вышеуказанными веществами и оборудованием допускается использовать с особенной осмотрительностью в дистанции наиболее 1 метра с СВТ и их соединительных проводов.

Осмотр СВТ обычно приводит к необходимости их изъятия для последующего экспертного исследования и(или) приобщения к делу в качестве вещественного доказательства.

В протоколе осмотра СВТ фиксируют:

- его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учетный номер изделия);

- тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов;

- состояние на момент осмотра (выключено или включено);

- техническое состояние - внешний вид, целостность корпуса, комплектность (наличие и работоспособность необходимых блоков, узлов, деталей, и правильность их соединения между собой), наличие расходных материалов, тип используемого машинного носителя информации;

- тип источника электропитания, его тактико-промышленные свойства и промышленное состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетного фильтра, количество присоединенного к нему электрооборудования, число питающих электрических разъемов розеток и т.д.);

- присутствие заземления («зануления») СВТ и его промышленное положение; присутствие и техническая вероятность включения к СВТ удаленного оснащения и(или) наиболее СВТ к этому оборудованию, или к каналу электросвязи; существующие повреждения, непредвиденные стандартом полезные перемены в архитектуре строения СВТ, его единичных элементов (Элементов, конструкций), в особенности те, которые имели возможность возникнуть в результате правонарушения, а в равной мере имели возможность вызвать формирование происшествия;

- следы преступной деятельности (следы орудий взлома корпуса СВТ, попадания вовнутрь корпуса, пальцев рук, несанкционированного подключения к СВТ посторонних технических устройств и др.);

- положение СВТ в месте, относительно периферийного оборудования и прочих электротехнических устройств;

- определенный порядок сочетания СВТ с иными промышленными приборами; группу возделываемой информации (всеобщего использования либо конфиденциальная);

- присутствие либо недостаток личных средств охраны осматриваемого СВТ и возделываемой в нем информации с неразрешенного допуска и манипулирования.

Если на момент осмотра СВТ находится в рабочем состоянии необходимо детально описать:

- расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве (экране, мониторе, дисплее);

- основные действия, производимые специалистом при осмотре СВТ (порядок корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения (или соединения) СВТ, отсоединения проводов, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.)[28].

Подготавливаясь к проведению обыска, дознаватель обязан разрешить что и в каком месте он будет отыскивать. С целью этого нужно тщательнейшим образом исследовать условия процесса и составить ориентирующую информацию о объекте обыска, участке его выполнения и личности обыскиваемого. Согласно процессам о правонарушениях в области компьютерной информации объектом обыска имеют все шансы быть не только лишь разнообразные СВТ, механические носители и содержащаяся на них компьютерная сведение, однако и бумаги, ресурсы электросвязи, созданные и адаптированные специализированные промышленные устройства, домашние электротехнические устройства и оборудование, материалы и приборы.

В процессе обыска необходимо сосредоточивать интерес на литературу, методичные вещества и маркетинговые проспекты согласно компьютерной

технике, обрабатыванию, охране, передаче и внегласному получению компьютерной информации, а кроме того в аудио-, видеокассеты, распечатки машинной информации и бумаги о подходящем образовании. Особенное внимание необходимо отдавать объектам, заключающим коды, пароли допуска, идентификационные номера, наименования, электрические адреса пользователей определенных компьютерных конструкций и сеток, методы входа и деятельность в режимах и сетях. Нужно кроме того переиллюстрировать записные (телефонные) книги, справочники и сборники, в том числе электронные, пребывающие в памяти телефонных агрегатов, пейджеров и прочих компьютерных девайсов.

Ценные свидетельства имеют все шансы быть выявлены и при личных обысках обвиняемых (подозреваемых).

Таковы главные характерные черты технологии и стратегии расследования компьютерных правонарушений в оперативно-розыскной деятельности работников ОВД.

Заключение

Таким образом выделить следующие общие группы компьютерных преступлений:

1) изъятие средств компьютерной техники;

2) перехват информации;

3) несанкционированный доступ к СКТ;

4) манипуляция данными и управляющими командами;

5) комплексные методы.

Компьютерные преступления весьма разнообразны и требуют постоянной и эффективной профилактики со стороны органов внутренних дел, так как предотвратить компьютерное преступление всегда намного легче и проще, чем его раскрыть и расследовать.

Выделяют три основные группы мер предупреждения компьютер-ных преступлений, составляющих в своей совокупности целостную систему борьбы с этим социально опасным явлением, а именно:

1) правовые;

2) организационно-технические;

3) криминалистические.

Наиболее эффективным направлением в предупреждении преступных посягательств является комплексное использование различных мер предупреждения компьютерных преступлений.

Однако одними мерами предупреждения не всегда удается предотвратить преступное посягательство. В связи с этим возникает необходимость заниматься не только вопросами защиты средств компьютерной техники, но и решать вопросы расследования компьютерных преступлений.

Раскрывать преступления в сфере компьютерной информации, сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место.

Для преступлений в сфере компьютерной информации типичны три ситуации первоначального этапа расследования:

1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствуют.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируют и осуществляют неотложные следственные действия, оперативно-розыскные, организационные и иные мероприятия, подробно рассмотренные в данной работе.

При наличии третьей следственной ситуации необходимоизучить поступившие материалы с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка их передачи в органы предварительного следствия. При необходимости - принять меры к получению недостающей процессуальной информации и провести иные следственные действия, перечисленные в данной

работе.
В очередность перечисленных следственных действий, оперативных и организационных мероприятий могут быть внесены коррективы в зависимости от изменения ситуации.

Все следственные действия по делам о преступлениях в сфере компьютерной информации проводятся в строгом соответствии с правилами, регламентированными действующим законодательством.

Список использованных источников

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (в ред. от 05.02.2014 № 2-ФКЗ) // Собрание законодательства Российской Федерации. 03.03.2014. № 9. Ст. 851.

2. Уголовно-процессуальный кодекс Российской Федерацииот 18 декабря 2001 г. № 174-ФЗ (в ред. от 21.07.2014) // Собрание законодательства Российской Федерации. 24.12.2001. № 52 (ч. I). Ст. 4921.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 21.07.2014) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

4. Федеральныйзакон РФ от 12 августа 1995 г. N 144-ФЗ«Обоперативно-розыскнойдеятельности» (в ред. от 21.12.2013)// Собраниезаконодательства РФ. 1995. № 33. Ст. 3349.

5. Федеральный закон РФ от 07.02.2011 № 3-ФЗ (в ред. от 21.07.2014) «О полиции» // Собрание законодательства РФ. 2011. № 7.Ст. 900.

Учебная и научная литература

6. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: Учебное пособие. М.: МАИК «Наука/Интерпериодика», 2012.

7. Бакотин А.С. Оперативно-розыскная деятельность: Учебное пособие. М.: Приор, 2012.

8. ВагинО.А., ИсиченкоА.П., ШабановГ.Х. Оперативно-розыскныемероприятияииспользованиеихрезультатов. М.: Издательский дом Шумиловой И.И., 2011.

9. Гульбин Ю.А. Преступления в сфере компьютерной информации: Учебное пособие. М.: «Статут» 2011.

10. Дубягин Ю.П., Дубягина О.П., Михайлычев Е.А. Комментарий к Федеральному закону «Об оперативно-розыскнойдеятельности». М.: Юстицинформ, 2011.

11. Коржов В.К. Право и Интернет: теория и практика: Учебное пособие. М.: Изд-во «БЕК», 2011.

12. Кочои С.Н. Ответственность за неправомерный доступ к компьютерной информации: Учебное пособие. М.: Изд-во РАГС, 2010.

13. КрыловВ.В. Информация как элемент криминальной деятельности: Учебное пособие. М.: ИНФРА-М, 2011.

14. Крылов В.В. Информационные преступления - новый криминалистический объект: Учебное пособие. 2011.

15. Крылов В.В. Информационные компьютерные преступления: Учебное пособие. М.: Юридическая литература, 2010.

16. Максимов В.Ю. Компьютерные преступления (вирусный аспект): Учебное пособие. М.: АО «Центр ЮрИнформ», 2011.

17. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011.

18. Панфилова Е.И. Компьютерные преступления: Учебное пособие. М.: Феникс, 2012.

19. Сальников В.П. Компьютерная преступность: Учебное пособие. М.: Приор, 2011.

20. Симкин Л.И. Компьютерное пиратство:Учебное пособие. М.: Статут, 2012.

21. Сухарев А. Компьютерные преступления: Учебное пособие. М : Приор, 2014.

1. Сухарев А. Компьютерные преступления: Учебное пособие. М : Приор, 2014. С.11. ↑

2. Крылов В.В. Информационные преступления - новый криминалистический объект: Учебное пособие. 2011. С.23. ↑

3. Крылов В.В. Информация как элемент криминальной деятельности: Учебное пособие. М.: ИНФРА-М, 2011. С.38. ↑

4. Панфилова Е.И. Компьютерные преступления: Учебное пособие. М.: Феникс, 2012. С.97. ↑

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 21.07.2014) // Собрание законодательства РФ. 1996. № 25. Ст. 2954. С.108. ↑

6. Крылов В.В. Информационные компьютерные преступления: Учебное пособие. М.: Юридическая литература, 2010. С.92. ↑

7. Сальников В.П. Компьютерная преступность: Учебное пособие. М.: Приор, 2011. С.71. ↑

8. Гульбин Ю.А. Преступления в сфере компьютерной информации: Учебное пособие. М.: «Статут» 2011. С.57. ↑

9. Коржов В.К. Право и Интернет: теория и практика: Учебное пособие. М.: Изд-во «БЕК», 2011. С.98. ↑

10. Максимов В.Ю. Компьютерные преступления (вирусный аспект): Учебное пособие. М.: АО «Центр ЮрИнформ», 2011. С.59. ↑

11. Кочои С.Н. Ответственность за неправомерный доступ к компьютерной информации: Учебное пособие. М.: Изд-во РАГС, 2010. С.102. ↑

12. Гульбин Ю.А. Преступления в сфере компьютерной информации: Учебное пособие. М.: «Статут» 2011. С.58. ↑

13. Симкин Л.И. Компьютерное пиратство: Учебное пособие. М.: Статут, 2012. С.40. ↑

14. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011. С.98. ↑

15. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: Учебное пособие. М.: МАИК «Наука / Интерпериодика», 2012. С.77. ↑

16. **Бакотин А.С. Оперативно-розыскная деятельность: Учебное пособие. М.: Приор, 2012. С.112.**

↑

17. Вагин О.А., Исиченко А.П., Шабанов Г.Х. Оперативно-розыскные мероприятия и использование их результатов. М.: Издательский дом Шумиловой И.И., 2011. С.80. ↑

18. Дубягин Ю.П., Дубягина О.П., Михайлычев Е.А. Комментарий к Федеральному закону «Об оперативно-розыскнойдеятельности». М.: Юстицинформ, 2011. С.50. ↑

19. Панфилова Е.И. Компьютерные преступления: Учебное пособие. М.: Феникс, 2012. С.103. ↑

20. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011. С.108. ↑

21. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: Учебное пособие. М.: МАИК «Наука / Интерпериодика», 2012. С.84. ↑

22. **Бакотин А.С. Оперативно-розыскная деятельность: Учебное пособие. М.: Приор, 2012. С.115.**

↑

23. Вагин О.А., Исиченко А.П., Шабанов Г.Х. Оперативно-розыскные мероприятия и использование их результатов. М.: Издательский дом Шумиловой И.И., 2011. С.81. ↑

24. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011. С.99. ↑

25. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: Учебное пособие. М.: МАИК «Наука / Интерпериодика», 2012. С.89. ↑

26. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011. С.100. ↑

27. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: Учебное пособие. М.: МАИК «Наука / Интерпериодика», 2012. С.90. ↑

28. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2011. С.101. ↑