Средства защиты информации

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

Процесс использования специальных знаний содействует более глубокому, всестороннему и оперативному исследованию условий и причин, способствующих совершению преступлений, что положено в основу предупреждения их совершения. Одним из направлений в процессе предупреждения преступлений является экспертная профилактика. Вся работа по экспертной профилактике строится на всестороннем и глубоком изучении и синтезе экспертного и судебно-следственного материала, причем, как отмечает Н.К.Ханджанов, серьезное значение здесь имеет статистическая обработка различных данных, в особенности учет и регистрация заключений экспертов. Однако в настоящее время все большую актуальность приобретает другое направление в профилактической деятельности экспертов – выработка новых методов выявления причин и обстоятельств, способствующих совершению преступлений и их предупреждению, а также новых направлений использования уже апробированных методик.

Как показывает анализ практики, наиболее распространенным преступлением в области высоких информационных технологий является неправомерный доступ к охраняемой законом информации. Причем первоначальной задачей предварительного расследования является установление факта несанкционированного доступа или же попытки незаконного проникновения в информационную систему. И здесь, как утверждают ученые, проблема сводится не только к взыванию к правосознанию жертв преступной деятельности, которые, своевременно подав заявление о преступлении, обеспечат наиболее оперативную, и как показывает практика, наиболее эффективную реакцию правоохранительных органов на преступные проявления, но и реализации комплекса профилактических мер.

В ходе рассмотрения современного состояния рынка информационных технологий нами было установлено, что в настоящее время имеет место внедрение и использование достижений науки и техники в данной области для обеспечения раскрытия и расследования преступлений. Однако данный процесс является взаимным, т.е. создаются разработанные на основе криминалистических методик идентификации технические продукты, используемые в различных ситуациях, в частности для предупреждения и профилактики совершения преступлений в сфере ВИТ. Одним из таких основных и приоритетных направлений, судя по широкому распространению неправомерного доступа к информации в общей качественной структуре преступлений, является профилактика несанкционированного доступа как одного из видов, т.е. защита информации.

Процесс профилактики в виде реализации защиты информации, как показывает практика, целиком и полностью зависит от тех лиц, которые владеют ей по роду своей служебной деятельности. Теоретически доказано, что можно обойти систему защиты любой программы, "взломать" ее. Существующее в науке криминалистике учение о совокупности индивидуальных признаков, позволяющих идентифицировать человека, и созданные на этой основе аппаратно-программные комплексы значительно повышают уровень безопасности данной информационной системы, причем в их основу положены биофизические, морфофункциональные и другие особенности строения человека. Внедрение в процессы изготовления и оперирования информацией таких комплексов носит прежде всего профилактический характер, так как основной их целью является организация таких условий, при которых невозможно осуществление неправомерного доступа к информации. Подобные аппаратно-программные комплексы, созданные на основе отдельных криминалистических методик идентификации человека, по нашему мнению, могут быть отнесены в раздел криминалистических средств защиты информации как одного из видов профилактики НСД.

Известно, чтобы получить доступ к системе, ее пользователь должен пройти два этапа. Первый – идентификация, при которой определяются те его характеристики, которых не имеют другие пользователи, второй – аутентификация, при которой происходит сверка определенного в ходе первого этапа пользователя с общим зарегистрированным списком пользователей, имеющих право доступа к системе. Но именно первый этап позволяет разработчикам систем защиты информации внедрить разработанные на основе криминалистических методик идентификации различных объектов аппаратно-программные комплексы.

Одной из наиболее простых и эффективных в реализации методик является проведение дактилоскопического исследования. В дактилоскопических устройствах защиты информации использованы высокие технологии идентификации личности, совмещенные с функциональностью и эргономичностью сканеров – устройств, с помощью которых происходит так называемое бескрасковое дактилоскопирование лица. Принцип действия сканеров заключается в том, что отраженный свет с поверхности отпечатка пальца проходит через призму и попадает на специальный датчик, который фиксирует четкое изображение папиллярного узора. Это высококонтрастное изображение, содержащее информацию о глубине и структуре рисунка, проходит процесс оцифровки, т.е. попадает в компьютер и сравнивается специально введенной программой с зарегистрированным ранее отпечатком. Доступ будет запрещен любому пользователю, чей отпечаток пальца не совпадет с зарегистрированным.

Более сложной в реализации является методика идентификации по структуре и взаиморасположению кровеносных сосудов руки, которая индивидуальна у каждого человека. Это продукты фирм «BK SYSTEMS Co. Ltd - ВК-300S», фирмы «Ethentica - Ethenticator MS3000» - сенсорная система проверки, включающая AuthenTec - аппарат, пропускающий через кончик пальца пользователя электрический ток очень малой мощности, создающий тем самым карту тканей из нескольких уровней, которая позволяет провести идентификацию даже в тех случаях, когда фаланги пальцев повреждены, и как отмечают разработчики, почти невозможно было бы установить при использовании обычного бескраскового дактилоскопирования - сканировании папиллярного узора. Особенностью данных устройств является то, что в процессе их работы происходит исследование внутренних органов человека - структуры кровеносных сосудов руки, их взаиморасположение, размеры и т.п., а не поверхности пальца, т.е. не отпечатка пальца с папиллярным узором. Таким образом, деформация поверхности, сухость, влажность или загрязненность рук никак не влияют на результаты идентификации.

Другим направлением в профилактике несанкционированного доступа путем использования криминалистических методик идентификации является реализация на аппаратно-программном уровне фонографического метода идентификации. Цель данного метода - установление личности по спектральным характеристикам голоса. Идентификация личности по голосу основана на том факте, что каждый человек обладает индивидуальным, только ему присущим комплексом фонетических и лингвистических признаков. Эти признаки зависят от его анатомических, психофизиологических и других социальных характеристик. Фонетические признаки в первую очередь поддаются спектральным исследованиям. Исследования в этой области начались еще тридцать – сорок лет назад. Обследования 25 тысяч человек, проведенные еще в 60-е годы американской телефонной компанией с помощью спектроанализатора голоса, дали коэффициент вероятности правильного обнаружения, равный 0.97, что является очень надежным показателем. Пример реализации данных положений в настоящее время - продукт компании «Vertiel – VoiceCheck», позволяющий идентифицировать пользователя посредством сопоставления произнесенной им конкретной фразы с образцами, имеющимися в системе в наличии (например, даже через телефонную линию, т.е. при наличии голосового модема, идентификация возможна и в сети Интернет).

Еще одним направлением использования положений криминалистической идентификации для профилактики несанкционированного доступа и обеспечения сохранности информации являются комплексы, основанные на портретной идентификации. Мы не будем останавливаться на тех экспертных методах, к которым относятся методы сопоставления, совмещения, наложения. Их можно считать традиционными (классическими). В связи с развитием вычислительной техники и вычислительной математики новый импульс совершенствования получили методы, позволяющие ввести в процесс исследования количественные характеристики. Так, в частности, было установлено, что если на сравниваемых изображениях запечатлено лицо в одном и том же положении, то идентификация личности может быть проведена на основании совокупности угловых измерений между наиболее представительными точками. Таких точек 14 на изображении лица в фас и 12 на изображении лица в профиль.

Некоторые другие методы, например аналитический метод идентификации, вероятностно-статистический метод, анализируют расстояния между выделенными на лице антропометрическими точками, вычисляют случайные ошибки и вероятностные оценки.

Однако следует отметить, что развитие методов с использованием количественных характеристик, основанных на выделении определенного количества антропометрических точек, зависит от успехов в нахождении и уточнении системы признаков на изображениях.

Одной из наиболее успешных реализаций указанного метода идентификации в целях профилактики преступлений является комплексная система «One-on-one Facial Recognition». Система основана на распознавании уникальных черт человеческого лица и позволяет контролировать доступ не только в информационную систему, но и в здание или помещение, где она расположена. Иными словами, происходит профилактика несанкционированного доступа не только на техническом, но и на организационном уровне ее реализации. Данный комплекс, используя видео- и цифровые камеры, распознает лица и обеспечивает так называемый «ненавязчивый» контроль над пользователем информационной системы. При первоначальной установке - инсталляции комплекса - пользователь должен зарегистрировать свое лицо в базе данных. В результате этой процедуры система «One-on-One» создаст цифровую подпись, связанную с изображением конкретного лица. При дальнейшем использовании комплекса, система будет идентифицировать изображение лица пользователя с хранящимися в базе. Как утверждают ее создатели, наличие косметики не влияет на работу системы распознавания в силу учета возможных ошибок в процессе идентификации. Такой аппаратно-программный комплекс идентифицирует людей даже в тех случаях, когда они решили отказаться от использования очков.

Еще одним направлением в нетрадиционной области использования габитоскопии является идентификация трехмерного изображения лица. Пример тому – Nvisage - разработка фирмы «Cambridge Neurodynamics». Уникальность продукта заключается в том, что он ориентирован на распознавание трехмерных объектов, в то время как в большинстве современных устройств используется только двухмерная техника. Двухмерные системы распознавания надежны при распознавании только в том случае, когда известен угол поворота головы и расстояния до глаз, рта, носа и т.д. Когда человек находится в движении, двухмерная система становится сильно зависимой от позы объекта распознавания. При использовании источников света для создания трехмерного изображения Nvisage может распознавать и более тонкие особенности лица.

Кроме того, создаются устройства, позволяющие идентифицировать человека по какому–либо одному признаку. Например, устройство EyeDentify’s ICAM 2001 использует камеру с сенсорами, которые с короткого расстояния (менее 3 см) измеряют свойства сетчатки глаза. Человеку достаточно взглянуть одним глазом в отверстие камеры ICAM 2001 и система принимает решение о праве доступа.

Наиболее сложным в реализации явился продукт, основанный на идентификации по почерку, в частности по подписи. Пример тому - eSign - программа для идентификации подписи, использующая специальную цифровую ручку и электронный блокнот для регистрации подписи. В процессе регистрации eSign запоминает не только само изображение подписи, но и динамику движения пера. eSign анализирует целый ряд параметров, включающих и общие признаки почерка конкретного лица:

- транскрипция подписи;

- вектор направления;

- данные о расположении цифрового пишущего прибора;

- динамика движения руки;

- ускорение;

- скорость;

- сила нажатия пишущего прибора;

- различные временные факторы.

Вместе с тем можно отметить тот факт, что существенным недостатком такой методики производства идентификации подписи является отсутствие приспособления к постепенному изменению лицом выработанности почерка, которым выполняется подпись, в силу постоянного развития его письменно-двигательного навыка и приспособления к условиям выполнения такой подписи.

Появляются и новые комплексы, основанные на псифизиологических особенностях работы за компьютером конкретного человека. Это, прежде всего, так называемая идентификация пользователя посредством его клавиатурного почерка - пакет ESL фирмы «Electronic Signature Lock». Он основаны на том, что работа на клавиатуре представляет собой последовательное нажатие и отпускание определенной совокупности клавиш. При заведении текстовой информации, как правило, осуществляется последовательное включение и выключение отдельных клавиш клавиатуры, что упрощает процесс фиксации и обработки временных параметров клавиатурного почерка.

В частности, при отработке метода верификации пользователя по набору одной и той же для всех пользователей ключевой фразы в качестве временных параметров клавиатурного почерка используются время удержания каждой из клавиш и паузы между нажатиями соседних клавиш. Если же фирма «Electronic Signature Lock» утверждает, что вероятность неверной идентификации пользователя при знании им правильного пароля менее 10-6. Учитывая, что манера клавиатурного почерка изменяется со временем, зависит от состояния здоровья и т.д., фирма утверждает, что используемые статистические алгоритмы столь изощренны, что позволяют учитывать эти неизбежные вариации. Созданная на основе разработанной российскими авторами методики идентификации экспериментальная программа обладает более высоким коэффициентом точности, так как по сравнению с аналогичными разработками зарубежных авторов она призвана своей конечной целью идентифицировать пользователя, а не верифицировать (выбрать одного из существующего списка пользователей), как предлагают другие, что в целом значительно снижает криминалистическую значимость их продуктов.

Это лишь часть из тех систем защиты информации, которые используют для идентификации личности биометрические характеристики конкретного человека в целях профилактики совершения им несанкционированного доступа. Указанные аппаратно-программные комплексы и системы в настоящее время имеются на рынке информационных товаров и услуг и доступны почти каждому человеку. Наличие такого рода комплексов, существенно повышает уровень защиты практически любой информационной системы и позволяет не только своевременно установить факт несанкционированного доступа, но и предотвратить его совершение, что является основной целью профилактики подобных преступлений. В ряде западных стран, например, некоторые банки пошли по оригинальному пути - используя подобные комплексы, компьютер разрешает доступ к информационной системе любому человеку (конечно, с ограниченным объемом прав пользования ею, хотя пользователь об этом не догадывается). Если в процессе идентификации пользователей произошли ошибки, т.е. в случаях, когда происходит попытка незаконного доступа, персонал банков уведомляет в данной ситуации правоохранительные органы, которые сразу же предпринимают попытку отслеживания пользователя, пытающегося проникнуть в систему, пока он еще находится в ней.

Как показывает практика, ущерб от совершения рассматриваемых преступлений во много раз превышает стоимость технических и организационных мер по осуществлению профилактики преступлений в сфере ВИТ вместе взятых. В связи с этим отказ от принятия организационных мер по защите информации по мотиву высокой себестоимости, является нецелесообразным.

Вместе с тем в науке уже выработан ряд организационных мер обеспечения защиты информации от несанкционированного доступа, преследующих профилактические цели:

- ограничение размеров сети - чем обширнее сеть, тем труднее организовать защиту информации в ней;

- изоляция сети от внешнего мира – ограничение физического доступа к сети извне уменьшает вероятность несанкционированного подключения. Это может выражаться в ограничении доступа путем физической или технической охраны коммутаторов, наземных антенн и других объектов, входящих в состав информационной сети;

- электронная цифровая подпись сообщений. На этом следует остановиться особо. В течение последнего времени происходит замена бумажной технологии обработки информации ее электронным аналогом, и, конечно, в будущем следует ожидать полного вытеснения бумажного документооборота электронным. Однако представление традиционных бумажных документов в виде электронных последовательностей, состоящих из нулей и единиц, обезличивает последние. Защитных атрибутов бумажных документов: подписей, печатей и штампов, водяных знаков, специальной фактуры бумажной поверхности и т.д., - у электронного представления документов нет. Но электронные документы необходимо защищать не менее тщательно, чем бумажные. Поэтому возникает задача разработки такого механизма электронной защиты, который бы смог заменить подпись и печать на бумажных документах. Т.е. необходимо разработать механизм цифровой подписи, которая представляет собой дополнительную информацию, приписываемую к защищаемым данным. Цифровая подпись зависит от содержания подписываемого документа и некоего секретного элемента (ключа), которым обладает только лицо, участвующее в защищенном обмене. Рассмотрим, в чем заключается этот механизм. Во-первых, цифровая подпись подтверждает, что подписывающее лицо не случайно подписало электронный документ. Во-вторых, цифровая подпись подтверждает, что только подписывающее лицо, и только оно, подписало электронный документ. В-третьих, цифровая подпись зависит только от содержания подписываемого документа и времени его подписания. В-четвертых, подписывающее лицо не имеет возможности впоследствии отказаться от факта подписи документах. Правовой основой использования электронно-цифровой подписи в документообороте на территории Казахстана является Закон РК «Об электронном документе и электронной цифровой подписи»;

- использование брандмауэров. Брандмауэр является вспомогательным средством защиты, применяемым только в том случае, если сеть нельзя изолировать от других сетей, поскольку брандмауэр довольно часто не способен отличить потенциально опасное сетевое сообщение от совершенно безвредного, в результате чего типичной будет ситуация, когда брандмауэр не только не защищает сеть от НСД, но и даже препятствует ее нормальному функционированию.

Рассмотренные организационные меры профилактики несанкционированного доступа могут быть применимы не только к компьютерным системам, но и к корпоративным системам сотовой связи и внутренних АТС предприятий и учреждений.

Суммируя вышеизложенное, можно констатировать тот факт, что интеграция положений различных видов криминалистической идентификации в область высоких информационных технологий обусловила возникновение новых технических способов и криминалистических средств для профилактики преступлений в сфере ВИТ, в частности защиты информации от неправомерного доступа. Возникли новые направления использования уже апробированных криминалистических методик производства идентификации, в том числе и для целей профилактики совершения подобных преступлений. НСД, являясь одним из распространенных видов таких преступлений, определил профилактику как наиболее приоритетное направление по предупреждению преступлений в сфере ВИТ, которое реализуется как в ходе технических, так и организационных мер по защите информации.