Содержание:

Введение

Все больше в прошлое уходит бесполезное нагромождение различных средств защиты, которое стало «модным» в результате реакции на первую волну страха перед компьютерными преступлениями. К тому, что защита информации должна носить комплексный характер, все начинают постепенно привыкать. При этом компании-заказчики больше не хотят выбрасывать деньги на ветер, они хотят приобретать только то, что им действительно необходимо для построения надежной системы защиты информации. Но организация обеспечения безопасности информации должна не просто носить комплексный характер, а еще и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты.

Процесс признания в России международных стандартов по защите информации не является обособленным исключительным решением, а становится естественной составной частью реформирования всей системы стандартизации.
В настоящее время в России наряду с отечественной нормативной базой широко используются около 140 международных стандартов в области информационных технологий, из них около 30 затрагивают вопросы защиты информации.

Одним из наиболее значимых является стандарт ИСО/МЭК 15408–99 «Критерии оценки безопасности информационных технологий», более известный как «Общие критерии». Этот стандарт дает новую методологию формирования требований по безопасности информационных технологий, отвечающих современному уровню их развития, и методологию оценки безопасности продуктов и систем информационных технологий.

Но вся идеология этого стандарта построена на необходимости глубокого изучения и анализа существующей обстановки и, особенно, выявлении актуальных угроз информационной безопасности. При этом должны быть оценены все угрозы, с которыми можно столкнуться, и выбраны только те, которые могут повлиять на безопасность информации. Стандарт предполагает, что при описании угроз должны быть идентифицированы источники этих угроз, методы воздействия, уязвимости, присущие объекту и многое другое.

Именно поэтому выбор правильной методологии оценки возможных угроз информационной безопасности является одним из основных направлений при переходе к международным требованиям.

Целью данной работы является рассмотрение угроз информационной безопасности и способов их реализации, анализ критериев уязвимости и устойчивости систем к деструктивным воздействиям.

Для достижения поставленной цели необходимо описать основные модели угроз безопасности систем и способов их реализации, системно анализировать критерии уязвимости систем к деструктивным воздействиям.

1. Определение сетевых атак

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:

В современных условиях ожесточенной конкурентной борьбы, компании, стремящиеся увеличивать свое влияния на рынке и формировать долгосрочные конкурентные преимущества должны ориентироваться на наиболее актуальные и эффективные методы ведения бизнеса и маркетингового продвижения. Одним из современных методов развития компаний и их брендов является создание и управление альянсами брендов, принцип которых основан на концепции конкурентного сотрудничества (co-petition).

Согласно предложенным во второй половине 1990-х годов принципам данного термина, конкурентное сотрудничество способно формировать принципиальные новые подходы к планированию стратегий бизнеса, в том числе, в сфере маркетинга. На современном этапе развития теории маркетинга особенно выделяют роль брендовых альянсов для расширения деятельности партнерских брендов, упрощенному процессу входа на новые потребительские и

технологические рынка, формирования лояльности потребителей и усиления собственного капитала бренда. Альянс брендов подразумевает взаимодействие двух или более брендов в краткосрочном или долгосрочном периодах, направленное на производство и выпуск на рынок новый продукт или услугу, как в физической (непосредственно продукт сотрудничества брендов) или в символической (совместная реклама) форме. Производным понятием брендового альянса выступает термин «ко-брендинг», характеризующий полное объединение маркетинговой деятельности брендов-партнеров, направленное именно на создание нового продукта.

Ежегодный рост товаров совместной деятельности брендов в США достигает порядка 20%, а, если рассматривать тенденции роста на мировой площадке, то данный показатель достигает 60% в год. Результаты исследований в области совместного брендинга иллюстрируют, что каждая из 500 крупнейших мировых организаций в среднем вступала в 60 альянсов с брендами других корпораций, однако успешное партнерство брендов достигалось лишь в 30% случаях.

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. Итак, рассматриваемая нами концепция создания брендового альянса для достижения конкурентных преимуществ компании в долгосрочной перспективе, с одной стороны, является новой и *актуальной методикой развития компании*, позволяет увеличить рыночную долю компании, повысить узнаваемость бренда и экономическую ценность. Однако с другой стороны, *стратегия объединения бренда в рамках альянса, способна разрушить существующее восприятия бренда в глазах потребителей, ухудшить имидж компании, не достичь поставленных целей и привести к большим финансовым потерям предприятия*. Поэтому крайне важно, в зависимости от целей компании прибрести выигрыш от альянса брендов в долгосрочном или краткосрочных периодах, учитывать влияние внешней и внутренней среды брендов, выбирать «правильных» партнеров для альянса и тщательно прорабатывать стратегию сотрудничества, основываясь на приобретении выгоды от альянса для всех партнерских брендов. Исходя из этого, выбор подходящего партнера для объединения брендов играет *критически важную роль для успешного партнерства на конкурентном рынке, учитывая все предпосылки деятельности альянса и сотрудничающих брендов.* 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 зарегистрирован В современных условиях ожесточенной конкурентной борьбы, компании, стремящиеся увеличивать свое влияния на рынке и формировать долгосрочные конкурентные преимущества должны ориентироваться на наиболее актуальные и эффективные методы ведения бизнеса и маркетингового продвижения. Одним из современных методов развития компаний и их брендов является создание и управление альянсами брендов, принцип которых основан на концепции конкурентного сотрудничества (co-petition).

Согласно предложенным во второй половине 1990-х годов принципам данного термина, конкурентное сотрудничество способно формировать принципиальные новые подходы к планированию стратегий бизнеса, в том числе, в сфере маркетинга. На современном этапе развития теории маркетинга особенно выделяют роль брендовых альянсов для расширения деятельности партнерских брендов, упрощенному процессу входа на новые потребительские и технологические рынка, формирования лояльности потребителей и усиления собственного капитала бренда. Альянс брендов подразумевает взаимодействие двух или более брендов в краткосрочном или долгосрочном периодах, направленное на производство и выпуск на рынок новый продукт или услугу, как в физической (непосредственно продукт сотрудничества брендов) или в символической (совместная реклама) форме. Производным понятием брендового

альянса выступает термин «ко-брендинг», характеризующий полное объединение маркетинговой деятельности брендов-партнеров, направленное именно на создание нового продукта.

Ежегодный рост товаров совместной деятельности брендов в США достигает порядка 20%, а, если рассматривать тенденции роста на мировой площадке, то данный показатель достигает 60% в год. Результаты исследований в области совместного брендинга иллюстрируют, что каждая из 500 крупнейших мировых организаций в среднем вступала в 60 альянсов с брендами других корпораций, однако успешное партнерство брендов достигалось лишь в 30% случаях.

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. Данная глава посвящена изучению теоритических основ процесса создания и управления брендовыми альянсами. В данной главе раскрывается определение и сущность понятий «бренд» и «ко-бренд», а также приводится генезис концепций изучения стратегических маркетинговых альянсов, охватывающие различные функциональные сферы организаций, как в коммерческом, так и в некоммерческом секторах. Также раскрываются предпосылки и мотивы создания маркетинговых альянсов, приводится описание и систематизация подходов, применяемых в изучении ко-брендинга. Для выявления роли брендового альянса и его значения на успешное функционирование хозяйственной деятельности организации в текущей главе особенно выделяется значение потребительской ценности в капитал бренда и рассматриваются понятия «капитал ко-бренда», «стоимость и сила ко-бренда», «эластичность ко-бренда». В конце обзора теоритической базы процесса ко-брендинга изучаются подходы к выбору партнера для создания и реализации успешного маркетингового альянса в процессе их становления в маркетинге. Далее приводится описание современных тенденций изучения альянсов бренда и выбора партнеров в соответствии с поставленными перед организацией целями. 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. Российский профессор в области маркетинга Д.А. Шевченко предложил следующее определение: «Бренд – знак, символ, слова или их сочетание, помогающие потребителям отличить товары или услуги одной компании от другой. Бренд воспринимается как широко известная торговая марка или компания, занимающая в сознании и психологии потребительских сегментов особое место из массы себе подобных».

Анализируя интерпретации приведенных выше определений, мы можем характеризовать *«бренд» как уникальное, единое обозначение (название, слоган, девиз, стиль, термин, идея), узнаваемое потребителем предложенного набора товаров или услуг.* Спектр товаров или услуг обычно объединяют по направлениям деятельности компании, для достижения экономической и стратегической эффективности. Согласно работе Валентина Перция и Лилии Мамлеевой «Анатомия Бренда», бренд - это выгода. Любая выгода - функциональная, эмоциональная, психологическая или социальная, которую покупатель получает вместе с приобретаемым товаром или услугой. Для того, чтобы бренд действительно достиг целевой аудитории, был узнаваем и нес за собой экономическую и стратегическую эффективность, крайне важно придерживаться фундаментальных направлений деятельности компании в отношении конкретного бренда. 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. По сути, бренд есть не материальное, а концептуальное понятие, которое направлено на достижение конкурентных преимуществ компании в конкретном секторе, целевой аудитории, формировании потребительской лояльности и прочих факторов для продвижения торговой марки на рынке. Для наиболее ясного объяснения концептуального понятия «бренд», разберем его по конкретизированным составляющим.

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. Одной из техник продвижения бренда является создание стратегического брендового альянса. В современном мире данный метод приобретает все большую популярность среди отечественных

и западных компаний. Брендовые альянсы можно рассматривать в качестве «мягкой формы» интеграции компаний, при которой фирмы обладают правовой и экономической независимостью.[1] Важно отметить, что данный альянс является промежуточной ступенью между слиянием компаний и их простым деловым взаимодействием.[2] Об этом в своих работах говорили такие ученые, как М. Портер [3], А. Томпсон и А. Стрикленд.[4] Более того, ученые отмечают, что стратегический брендовый альянс есть ни что иное как возможность сотрудничать и конкурировать с другими компаниями одновременно.[5]

Данный парадокс получил в английском языке название «co-petition» - конкурентное взаимодействие. Впервые процесс конкурентного взаимодействия был описан в работе А. Бранденбургера и Б. Нейлбаффа 1996 года, которые утверждали, что в бизнесе одновременно сосуществуют и конкуренция, и кооперация. Более того, правильное использование данных механизмов способно в итоге привести к выигрышу несколько взаимодействующих компаний.[6] Интересен тот факт, что в рамках традиционных подходов конкуренция и кооперация рассматривались в качестве противопоставляющийся понятий, не способных к совместному существованию.

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.

Многие ученые писали о сложности ведения конкурентной борьбы и о необходимости овладения инструментами ее ведения с целью победы над основными конкурентами.[7] Данная парадигма была достаточно строгой: один из конкурентов будет победителем, тогда как остальные – проигравшими. Необходимо отметить, что в данных условиях успешная практика конкурентного взаимодействия говорит о том, что столь жесткое противопоставление конкуренции и кооперации не всегда уместно и следует обратить внимание на существование феномена «co-petition». Данный термин имеет множество вариантов перевода среди российских ученых. Встречаются такие обозначения, как «коокуренция», «конкоперация», «коопкуренция», «кооперенция», «сотруенция» и «соткуренция». Также существует большое количество определений данного понятия. Одно из них, наиболее полно охватывающее область конкурентного взаимодействия компаний выглядит следующим образом. Коопетиция - концепция, нацеленная на преодоление упрощенного взгляда, основанного на традиционных подходах к конкуренции и кооперации. Предлагает описание более сложных структур рынка, где сотрудничество и конкуренция сливаются вместе с целью формирования новой концепции, в большей степени соответствующей сложности «ролей», стратегий, форм поведения и целей акторов на современном рынке.[8] Таким образом можно говорить о том, что стратегические альянсы являются результатом нетрадиционного взаимодействия фирм, основанного на соединении конкурентных и кооперативных черт, и потому требуют более детального изучения. 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. Что касается предпосылок возникновения маркетинговых альянсов, то здесь можно говорить о том, что подходы к их формированию зависят во многом от разных областей взаимодействия компаний. Ими могут являться маркетинг, финансы, производственные процессы, НИОКР, логистика, а также человеческие ресурсы. В указанных направлениях наблюдается расширение взаимодействия компаний в рамках стратегических альянсов. Поэтому к стратегическим альянсам можно отнести маркетинговые альянсы, альянсы в производственной и научно-технической сфере. При этом важно упомянуть о важной роли маркетинговых стратегических альянсов. Именно их создание способствует длительным стратегическим успехам организаций. 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.

2. Методы защиты информации

Проблема создания системы защиты информации включает две взаимодополняющие задачи:

1) разработка системы защиты информации (ее синтез);

2) оценка разработанной системы защиты информации.

Вторая задача решается путем анализа ее технических характеристик с целью установления, удовлетворяет ли система защиты, информации комплексу требований к данным системам. Такая задача в настоящее время решается почти исключительно экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Рассмотрим основное содержание современных методов защиты информации, которые составляют основу механизмов защиты.

Препятствия — методы физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

Управление доступом - метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

• идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

• опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

• проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• регистрацию (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка — метод защиты информации путем ее криптографического закрытия. Этот метод широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

Регламентация — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение — метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных). [12,с.325]

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких, как технические, программные, организационные, законодательные и морально-этические. К. основным **средствам защиты,** используемым для создания механизма обеспечения безопасности, относятся следующие:

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под **аппаратными средствами** принято понимать технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Например, система опознания и разграничения доступа к информации (посредством паролей, записи кодов и другой информации на различные карточки).

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, источники бесперебойного питания, электромеханическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации. В такую группу средств входят: механизм шифрования (криптографии — специальный алгоритм, который запускается уникальным числом или битовой последовательностью, обычно называемым шифрующим ключом; затем по каналам

связи передается зашифрованный текст, а получатель имеет свой ключ для дешифрования информации), механизм цифровой подписи, механизмы контроля доступа, механизмы обеспечения целостности данных, механизмы постановки графика, механизмы управления маршрутизацией, механизмы арбитража, антивирусные программы, программы архивации (например, zip , rar, arj и др.), защита при вводе и выводе информации и т. д.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, использование, эксплуатация).

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их обычно ведет к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. [13,с.312]

Все рассмотренные средства защиты разделены на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

3. Примеры угроз информационной безопасности

По результатам исследования «Лаборатории Касперского» в 2015 году 36% российских пользователей минимум один раз пострадали от взлома аккаунта, в результате чего были украдены их персональные данные, либо профиль был использован для рассылки вредоносного ПО.

Чаще всего злоумышленников интересует доступ к аккаунту в социальной сети и электронной почте (14%) и пароль к онлайн-банкингу (5%).

53% респондентов в результате взлома получили фишинговые сообщения или попали на подозрительные сайты, целью которых было вытягивание из них учетных данных. В качестве определения стратегического альянса было предложено следующее: партнерство фирм и/или общественных институтов, развивающих маркетинговые инициативы, связанные с организацией, контролем и реализацией совместных маркетинговых программ для достижения общих или независимых, но совместимых целей через удовлетворение потребителей. Основным отличием подхода в рамках ко-маркетинга от подхода маркетинга взаимоотношений являлось более четкое определение состава участников альянса. Также стратегический маркетинговый альянс стал рассматриваться в качестве возможности для компании по расширению своей деятельности без изменения ключевых компетенций.

Страдают от действий киберпреступников не только сами пользователи, чьи учетные данные были украдены, но также их друзья и родственники. Так, более половины жертв взлома аккаунта обнаружили, что кто-то рассылал сообщения от их имени, и почти каждый четвертый - что их друзья кликнули на полученную от них вредоносную ссылку.

Несмотря на это, только 28% пользователей создают надежные пароли для своих аккаунтов и только 25% выбирают безопасные способы их хранения.

За год с июня 2014 года по июнь 2015 года киберпреступники через системы интернет-банкинга в рунете похитили 2,6 млрд руб., следует из отчета компании Group-IB на конференции "Тенденции развития преступлений в области высоких технологий-2015". За аналогичный период прошлого года сумма была в несколько раз выше - 9,8 млрд руб. "Мы фиксируем снижение ущерба при росте количества атак",- уточнил руководитель сервиса киберразведки Bot-Trek Intelligence Дмитрий Волков.

Наибольший ущерб понесли юридические лица, лишившиеся в результате действий киберпреступников 1,9 млрд руб. На данном этапе развития

маркетинговый альянс можно было определить, как партнерство организаций, нацеленное на создание товаров, находящихся на стыке различных рынков и продуктовых категорий, не имеющих очевидной связи друг с другом, с целью реализации маркетинговых инноваций. Именно поиск возможностей для роста вне основного рынка компании стал основным двигателем создания стратегических маркетинговых альянсов в начале двадцать первого века. Хакеры при этом научились обходить традиционные средства защиты: ни токены, ни дополнительная SMS-аутентификация не спасают от «автозаливов» - троянов, позволяющих переводить деньги со счетов посредством подмены реквизитов. Подтверждая платеж, клиент, зараженный таким трояном, видит правильные данные получателя, хотя в реальности деньги уходят на счет злоумышленников.

Сами российские банки в результате целевых атак за отчетный период потеряли 638 млн. руб. Даже единичные атаки на клиентов крупных банков приносят большой доход. Усиливается интерес злоумышленников и к торговым, и к брокерским системам. Так, в феврале 2015 г. была проведена первая в России успешная атака на биржевого брокера, длившаяся всего 14 минут и приведшая к ущербу около 300 млн. руб.

Почти 100 млн. руб. похищено у физических лиц, причем 61 млн руб.- с помощью троянов, заточенных под платформу Android. Уязвимость Android привлекает все больше злоумышленников, следует из отчета: появилось десять новых преступных групп, работающих с Android-троянами, а количество инцидентов выросло втрое.

Она подразумевает под собой ориентацию не только на извлечение прибыли для компании, но и на акцентировании деятельности фирмы на проблемах глобального развития. [9] В этих условиях роль стратегических маркетинговых альянсов существенно возрастает. На данном этапе формирования маркетинговой концепции стратегический маркетинговый альянс есть ни что иное как сообщество лояльных партнеров, объединенных общим видением, миссией и ценностями, целью которого является не только получение прибыли, но и улучшение современного глобализованного мира. Ежедневно 70 пользователей мобильных банков на Android становятся жертвами киберпреступников.

По данным Group-IB, продолжается развитие экосистемы, обслуживающей совершение киберпреступлений. Услуги по обналичиванию похищенных денег принесли злоумышленникам 1,92 млрд. руб. Растет оборот площадок, торгующих данными о банковских картах, логинах и паролях разных систем: выручка семи таких магазинов превысила 155 млн. руб.

Согласно прогнозу, в следующем году разработчики вредоносного софта полностью сосредоточатся на мобильных платформах, число инцидентов и суммы хищений у физических лиц увеличатся за счет перехвата на Android-устройствах данных карт, логинов и паролей для интернет-банкинга. Для большинства потребителей бренд предстает совершенно исключительным образом, ведь человек даже готов отдать за него большие деньги, выделяя конкретный товар или услугу среди других. То, что общественность готова выделять из своих средств сумму, которая превышает стоимость схожих продуктов, говорит о том, что правильное брендирование делает предложение максимально привлекательным. По своей природе любой человек не будет принимать простые решения, связанные с тратой его ресурсов. Любая покупка решает какую-либо проблему потребителя, удовлетворяет определенную потребность. Вырастет и количество хищений информации о банковских картах через POS-терминалы: появляется все больше программ для этих целей, а часть из них находится в открытом доступе.

Согласно исследованию ИБ-компании Invincea, за последние несколько дней эксперты обнаружили 60 случаев инфицирования систем банковским вредоносным ПО Dridex на территории Франции. Вредонос распространяется под видом электронных писем с вложенным файлом Microsoft Office, который выглядит, как счет из популярного отеля или магазина. Вредоносное вложение оформлено на французском языке и содержит шестнадцатеричный код.

В 2014 году почти 18 млн американских граждан стали жертвами хищения личности, причем в большинстве случаев целью злоумышленников были кредитные карты и банковские счета, сообщает издание The Networkworld со ссылкой на отчет Министерства юстиции США.

По данным Бюро юридической статистики (Bureau of Justice Statistics), за последний год число жертв кибермошенников увеличилось на 1 млн. по сравнению с показателем 2012 года. Стоит отметить, что в отчете ведомства учитывались не только случаи компрометации персональной информации, но и использование ее для получения финансовой или иной выгоды. Согласно данным, два из пяти инцидентов были связаны с незаконными манипуляциями с кредитными картами, и примерно такое же количество – с махинациями с банковскими счетами.

В исследовании «Финансовые последствия киберпреступлений» за 2015 г., проведенном Ponemon Institute (США), представлены данные о ежегодных затратах на устранение последствий кибератак для компаний в США, Великобритании, Японии, Германии, Австралии, Бразилии и России.

Известно, что основное решение о покупку товара принимается на эмоциональном уровне. Эмоции провоцируют спонтанное и импульсивное решение о покупке, в то время как рациональность тяготеет к анализу, что может быть причиной отказа от покупки. Покупатель выбирает продукт не всегда качественный, но продукт, к которому он чувствует «предрасположенность». Поэтому на рынке идет «борьба» за наиболее выигрышное восприятие потребителей бренда компании. США в год – то есть на 82% больше, чем на момент начала исследования шесть лет назад. Иными словами, каждый год затраты увеличивались почти на 20%.

На ликвидацию последствий кибератак сегодня требуется в среднем 46 дней (за шесть лет этот срок увеличился почти на 30%), причем на устранение последствий каждой из них компании тратят в среднем по 1,9 млн долларов США.

Исследование в США показало также, что многие предприятия, чтобы избежать затрат, связанных с обнаружением кибератак и устранением их последствий, вкладывают средства в технологии аналитики в сфере безопасности. Такая тактика приносит плоды: затраты на реагирование на атаки сокращаются, и это позволяет существенно увеличить окупаемость инвестиций.

Личные данные 1,5 млн пользователей оказались опубликованными в облачном сервисе Amazon

Жертвами утечки стали клиенты организаций, занимающихся медицинским страхованием.

Полтора миллиона американцев стали жертвами утечки персональной информации. Полные имена, адреса, номера телефонов, данные о состоянии здоровья и прописанных медикаментов по ошибке были опубликованы в открытом виде в облачном сервисе Amazon компаниями, занимающимися медицинским страхованием и использующим программное обеспечение Systema Software.

Инцидент затронул Фонд самострахования Канзаса, страховую компанию CSAC Excess Insurance Authority и базу данных округа Солт-Лейк в штате Юта. Причина утечки и точное количество пострадавших пока неизвестны.

Но, несмотря на то, что история бренда множественными примерами подтверждает правомерность такого подхода, вопрос остается открытым. Потому, что эмоциональная реакция на покупку преобладает у детей, у женщин, у взрослых с серьезными когнитивными отклонениями. Кроме того, решение на что больше воздействовать - на сердце или разум потребителя зависит от особенностей

продукта. Там, где ценность бренда заключена в его функциональных преимуществах таких как, ассортимент, качество, следует апеллировать к разуму покупателя, а там, где бред приобретают для демонстрации социального статуса, взывать следует к эмоциям.В общей сложности были опубликованы номера социального страхования 1 млн. пользователей, 5 млн. записей о финансовых транзакциях, данные о сотнях тысяч полученных травм и 4,7 млн. примечаний, в том числе касающихся расследований случаев мошенничества

Заключение

Важно знать, что характерной особенностью электронных данных является возможность легко и незаметно искажать, копировать или уничтожать их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию. Защищённой называют информацию, не изменившую в процессе передачи, хранения и сохранения достоверность, полноту и целостность данных.

Несанкционированные воздействия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью разных методов воздействия. Подобные действия могут быть обусловлены стихийными бедствиями (ураганы, ливни, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с ними обычно весьма затруднена из-за в значительной степени непредсказуемости таких воздействий.

Наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Для защиты информации в компьютерах и информационных сетях широко используются разнообразные программные и программно-технические средства защиты. Они включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения. Для защиты информации от утечки в компьютерных сетях используют специальное техническое средство – Firewalls, располагаемое между внутренней локальной сетью организации и Интернетом. Другим устройством эффективной защиты в компьютерных сетях является маршрутизатор. Он осуществляет фильтрацию пакетов передаваемых данных и, тем самым, появляется возможность запретить доступ некоторым пользователям к определённому “хосту”, программно осуществлять детальный контроль адресов отправителей и получателей и др.

Охрана и безопасность объектов, людей и информации достигается взаимодействием специальных радиоэлектронных приборов, устройств и электрооборудования, в т.ч. пожарной и охранной сигнализации, средств технической и инженерной защиты, специально подготовленного персонал и транспорта. В качестве технических средств используются решётки на окна, ограждения, металлические двери, турникеты, металодетекторы и др.

К наиболее практикуемым способам защиты информации относится её кодирование, предполагающее использование криптографических методов защиты информации. Оно не спасает от физических воздействий, но в остальных случаях служит надёжным средством. Другой метод предполагает использование устройств, ограничивающих доступ к объектам и данным. Ведущее место среди них занимают биометрические системы. Они позволяют идентифицировать человека по присущим ему специфическим статическим и динамическим признакам (отпечаткам пальцев, роговице глаза, форме руки, лицу, генетическому коду, запаху, голосу, почерку, поведению и др.).

Комплексно мероприятия по обеспечению сохранности и защиты информации, объектов и людей включают организационные, физические, социально-психологические мероприятия и инженерно-технические средства защиты.

Список используемой литературы

1. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. 1999.
2. IBM Internet Security Systems [Электронный ресурс] – Режим доступа: [http://www.iss.net] (дата обращения: 20.01.2017).
3. Nessus [Электронный ресурс] – Режим доступа: [http://www.tenable.com/products/nessus] (дата обращения: 20.01.2017).
4. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений / Н.Г. Милославская, А.И. Толстой. – М.:ЮНИТИ-ДАНА, 2001. – 592 с.
5. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13.
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с.

7. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] (дата обращения: 21.01.2017).
8. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] (дата обращения: 21.01.2017).
9. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с.
10. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.:Питер, 2012. — 960 с.

1. Владимирова И.Г. Организационные формы интеграции компаний // Менеджмент в России и за рубежом. 1999. -No6. -С. 113-129. ↑

2. Зобов А. М. Методологические проблемы классификации стратегических альянсов // ЭСНР. - 2005. —No 4(31). -С. 147. ↑

3. Портер М Международная конкуренция. - М: Международные отношения, 1993. - С.86. ↑

4. Томпсон А.А., Стрикленд А. Дж. Стратегический менеджмент. Искусство разработки и реализации стратегии. - М.,2000. - 576 с. ↑

5. Капферер Ж. Н. Бренд навсегда. - М.: Вершина, 2007. - 4 4 8 с. ↑

6. Brandenburger A., Nalebuff B. Co-opetition: Revolutionary Mindset that Redefines Competition and Cooperation: The Game Theory Strategy that's Changing the Game of Business. - NY: Doubleday, 1996. - 290 p. ↑

7. Траут Дж. Сила простоты. -С.-Пб. Питер, 2001. -С.65. ↑

8. European institute for advanced studies in management (EIASM),2008 ↑

9. Никишкин В.В. Инновационная концепция маркетинга как ответ на вызовы современного мира // Практический маркетинг. -2011. - No 12(178).-С.4-7. ↑