ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТ

Описание проблемы

Сайту, порталу и виртуальному центру данных нужна надежная система безопасности. По мере того как компания двигается в направлении распределенной обработки данных и упрощения доступа к информации, угрозы безопасности приобретают все более масштабный характер. Сочетание этих факторов способствует усилению риска. Необходима система комплексного управления безопасностью (КУБ). Нужно решить, какая роль будет отводиться управляемым службам безопасности и как совладать с нарастающим потоком данных, поступающих от средств защиты. Прибавьте сюда постоянные обновления программного обеспечения и проблемы, связанные с беспроводными системами.

Лишь три процента веб-приложений достаточно надежны, чтобы противостоять хакерам, 97% веб-сайтов имеют "серьезные дефекты в защите", в результате чего данные и системы могут быть взломаны с целью злонамеренного использования. Из 97% обнаруженных серьезных "дыр" почти 40% приложений позволяли взломщикам получать полный контроль и доступ к информации. Около 23% дефектов могли привести к нарушениям конфиденциальности, а 21% обнаруженных ошибок давали возможность "похищать" товары из электронных магазинов. 5% дефектов позволяли взломщикам изменять информацию, а еще 5% - перехватывать транзакции. 2% ошибок в программном обеспечении настолько серьезны, что злоумышленники могут преспокойно удалить веб-сайты.

В развитых странах предприятия расходуют на обеспечение информационной безопасности от 5 до 7% бюджета, отведенного на информационные технологии. В России же компании тратят на эти цели куда меньше — лишь 1-2%

В России приблизительно 48% компаний используют антивирусное программное обеспечение. Вторыми по популярности (около 29%) являются межсетевые экраны и средства построения виртуальных частных сетей (VPN). Примерно одинаковое количество финансовых средств тратится на решения для обнаружения атак (10%) и продукты для идентификации, авторизации и администрирования (11%). В Европе же наибольшее внимание уделяется как раз средствам идентификации, авторизации и администрирования. **Рекомендуется защищаться не от угроз «вообще», а от риска простоя** информационной системы.

Совершенствуется не только защита, но и нападение. Атаки вирусов становятся комплексными — они распространяются несколькими путями и вред наносят разнообразный: крадут почтовые адреса, блокируют работу некоторых программ, оставляют лазейки для последующих нападений.

В **80% случаев сбои в работе ИТ-систем происходят на программном уровне**, то есть из-за программных ошибок, проникновения в систему вирусов, повреждения данных, случайного их удаления и т. д. В 12% случаев простои происходят из-за отказа аппаратных компонентов системы. Причиной еще 8% сбоев являются различные природные катаклизмы, террористические акты, проблемы с электропитанием.

Угрозу для жизнеспособности бизнеса, даже большую, чем терроризм, представляют ошибки или злонамеренные действия сотрудников. Ситуация усугубляется зачастую излишне легкомысленным отношением предприятий к планам по аварийному восстановлению данных. Так, 17% **ИТ-менеджеров вообще не имеют плана аварийного восстановления**, 57% пересматривают такой план раз в год и реже, 6% — никогда их не пересматривают, а 25% — никогда не тестировали подобные планы.

С простоями вычислительной техники сталкивались 84% всех предприятий. В 26% из них сбои случаются один раз в квартал и чаще. В 14% предприятий продолжительность простоя системы составила от 24 до 48 часов; в 16% — наблюдались потери важных данных.

Влияние нарушений безопасности на деятельность ИТ служб представлено в Табл. 1

Таблица 1

Влияние нарушений безопасности на деятельность ИТ служб

Испорченные, потерянные и недоступные хранимые данные	29%
Недоступные электронная почта и приложения	26%
Неработоспособность сетей	24%
Финансовые потери	5%
Негативное влияние на репутацию торговой марки	4%
Кража интеллектуальной собственности	4%
Нарушение закона	3%
Мошенничество	3%
Кража личной информации (о клиентах или сотрудниках)	3%
Падение цены акций	1%
Вымогательство	1%

Необходимость обеспечения безопасности данных связана со следующими причинами:

- Н**епосредственными расходами на восстановление и простой.** Эти расходы наиболее существенны и могут быть очень значительными. Сюда же следует отнести расходы на уменьшение работоспособности (например, система устояла, но канал связи оказался забит запросами атакующего) и расходы на отвлечение персонала от их основной работы (крупные сбои могут привлечь на борьбу и восстановление большую часть персонала компании).

- **Снижением доверия клиентов**. Крупные сбои не удастся скрыть от общественности, а это создает опасность, что клиенты перейдут к конкуренту, а значит потерю прибыли.

- **Опасностью судебного преследования**. Потеря денег клиентов или разглашение частной информации, может привести к судебному разбирательству, а значит потерям на судебные издержки, а возможно и крупные компенсации.

- **Собственно потерей и/или разглашением секретных данных**. Не поддается оценке, ущерб просто может быть огромен, вплоть до банкротства фирмы.

Инвестиции организаций в обеспечение информационной безопасности в виде приобретаемых средств защиты, затрат на оплату труда специалистов, на проведение внешнего аудита безопасности и т. п., неуклонно увеличиваясь из года в год, зачастую не окупаются. Происходит это главным образом потому, что большинство организаций продолжают придерживаться фрагментарного подхода, который оправдывает себя только при слабой зависимости организации от ИТ и низком уровне рисков информационной безопасности. Адекватный уровень информационной безопасности в состоянии обеспечить только комплексный подход, предполагающий планомерное использование как программно-технических, так и организационных мер защиты на единой концептуальной основе. При этом организационные меры играют первостепенную роль. Эффективность самых сложных и дорогостоящих механизмов защиты сводится к нулю, если пользователи игнорируют элементарные правила парольной политики, а сетевые администраторы нарушают установленные процедуры предоставления доступа к ресурсам корпоративной сети.

Возможные нарушения безопасности – реальные угрозы

Перехват. Хакерам легче всего заполучить имена сообществ с правами чтения: одной программы-анализатора (наподобие Ethereal) достаточно для чтения запросов от менеджеров управления сетью. Системы, где для защиты доступа не применяются списки контроля доступа, легко становятся жертвами хакеров. Но и защита с помощью списков доступа часто бывает мало эффективной из-за ошибок реализации. Нечистые на руку сотрудники могут обходить списки.

Подбор имени сообщества/метод «грубой силы». Значительный фактор риска представляют собой не удаленные имена сообществ по умолчанию. В Internet можно найти довольно полные списки, на основании которых легко подобрать имена по умолчанию к системам практически любого производителя. Часто администраторы оставляют эти имена после инсталляции, что существенно облегчает хакеру захват систем. Системы сканирования защиты предлагают легко реализуемую атаку на системы SNMP, в рамках которой в процессе подбора имени сообщества, наряду со списками слов, перебираются все доступные последовательности знаков. Если у хакера есть время (несколько недель), то он может провести такую атаку методом «грубой силы» и без заметного увеличения нагрузки на сеть. Однако подобные действия должны распознаваться всякой хорошо сконфигурированной системой обнаружения несанкционированного доступа.

Перехват через систему удаленного мониторинга. Удаленный мониторинг разрабатывается с целью дистанционного анализа сети и нахождения неисправностей и, при условии разумного использования, значительно облегчает обслуживание компьютерной сети. При этом предоставляется справка о компьютерах в сети (hosts), отправителях и получателях наибольшего объема данных (hostTopN, как правило, серверы) и т. п. Нередко «перевербованные» коммутаторы или маршрутизаторы в течение нескольких месяцев используются в качестве исходной базы для хакеров. Так ли уж часто администратор проверяет конфигурацию коммутатора, если он функционирует без сбоев?

Другие атаки. В инструментах управления того или иного производителя можно всегда найти слабые места из-за ошибок реализации. При этом возникает целый ряд проблем безопасности, из-за которых становится возможным доступ к конфигурационным данным, содержащим имена пользователей, пароли и имена сообществ. Излюбленный прием взломщика — переконфигурация маршрутизаторов. Он может контролировать обмен данными с целью их изменения или только считывания и создавать таким образом условия для технически сложных атак с промежуточным звеном (Man in the Middle), при которых он указывает свой маршрутизатор в качестве еще одного пункта следования пакетов на пути между сервером и жертвой.

Коммутаторы позволяют осуществлять анализ через зеркальные порты. В таком случае хакеру удается получить доступ практически ко всем передаваемым коммутатором данным. Единственное условие — достаточная пропускная способность зеркального порта.

Следует также упомянуть имеющиеся почти в любом программном обеспечении уязвимости вследствие переполнения буфера. Хакеры используют ошибки программирования путем ввода сверхдлинных последовательностей знаков, которые приводят либо к сбою

соответствующего процесса/системы, либо к исполнению недопустимых шагов программы на атакованной системе. Особенно много найдется таких уязвимых мест у сконфигурированных через сервер Web маршрутизаторов.

Источники «информационных катастроф» являются: неверная, неполная, бесполезная информация, информационная перегрузка.

Технологии развиваются, и инструментарий, который может использоваться для атак на системы, по своим возможностям всегда будет опережать продукты, предназначенные для их защиты. И помните: только хорошо обученные, квалифицированные пользователи, осознающие важность этой проблемы, смогут поддерживать целостность и защиту информации и ресурсов перед лицом постоянно растущей угрозы.

Анализ уязвимости бывает двух видов: пассивный и активный. При пассивном подходе производится сканирование системы, делая предположение о возможности проведения вторжения. А активный подход предполагает попытки проведения контратаки.

Оценка рисков нарушений безопасности

При разработке любой стратегии защиты, прежде всего, необходимо точно определить, что именно надо защищать. Начните с выяснения реальных ограничений систем, безопасность которых вы намерены обеспечить. ИТ-системы представляют собой комплексы физических компонентов, программного обеспечения, данных, служб связи и бизнес-процессов. Важно отметить, что система вовсе не обязательно состоит из компьютеров, связанных друг с другом или с чем-то еще. Например, у каждого из разъездных агентов есть свой мобильный компьютер, все эти компьютеры служат для выполнения одной и той же работы и контролируются уполномоченным на это специалистом. Все мобильные компьютеры тоже следует защищать.

После того, как вы выяснили, что представляет собой система, которую вам предстоит защитить, вы можете лучше понять, кто и что ей угрожает. Теперь нужно определить, насколько важен каждый из компонентов для решения того круга задач, которые стоят перед данным подразделением. Информация, хранящаяся в системе, физическая инфраструктура, программное обеспечение и специалисты, работающие с данной системой, должны оцениваться с точки зрения трех основных типов потенциальных угроз — тех, что приводят к снижению готовности, надежности и к раскрытию секретной или конфиденциальной информации.

При оценке риска достаточно получить объективные ответы на три следующих вопроса. **Насколько важен конкретный ИТ-ресурс?** Какой вред будет нанесен организации в том случае, если данный ресурс окажется поврежден или уничтожен? Какова вероятность того, что злоумышленники смогут и будут использовать данное уязвимое место для своих атак?

Риск — это возможность появления убытков, которая возникает как результат взаимодействия пары «угроза» и «уязвимость». Для каждой угрозы требуется оценить убытки, которые будут иметь место при ее реализации. Таким образом, требуется знать стоимость замены, возможные затраты на воссоздание интеллектуальной собственности, стоимость часа машинного времени, другие условия (во что обойдется утрата конфиденциальности, целостности и т. д.).

Следует отметить, что процесс оценки рисков включает три трудоемкие работы: идентификация ресурсов и определение их стоимости; выявление угроз; определение контрмер. Сроки выполнения каждой из них могут быть достаточно велики. Не рекомендуется пытаться снизить требуемые трудозатраты на оценку рисков и тем самым сократить сроки: это может повлечь неточности при формировании перечня ресурсов и соответствующих угроз.

К макрообъектам применимы в основном макроугрозы, в частности стихийные бедствия. Как правило, такие риски передаются страховым компаниям.

Сетевые фильтры могут вследствие перегрузки повредить оборудование. Утечки наполнителя огнетушителей и аккумуляторов плохо влияют на электронику; часто оборудование сильно зависит от сопутствующих систем кондиционирования. Следует также рассматривать возможность кражи оборудования или его использования в несанкционированных целях.

Программные продукты могут быть случайно либо намеренно изменены или уничтожены самими программистами или пользователями. Как ни странно, но процесс создания резервных копий также несет в себе угрозы нарушения работы программного обеспечения. Как правило, это связано с неотлаженной процедурой восстановления информации из резервных копий. Имеется и определенный риск, что устанавливаемое программное обеспечение изначально является поврежденным и неработоспособным, в то время как предыдущая рабочая версия уже затерта.

Следует изучить, как обеспечивается безопасность хранения носителей и могут ли они быть повреждены или утеряны. При утере носителя следует принять во внимание также ценность информации, хранящейся на данном носителе.

Применительно к данным учитываются угрозы, создаваемые злоумышленниками. Информация на диске может быть скопирована, считана или даже затерта через сетевые соединения. Носители (внешние копии, распечатки, а также сами компьютеры) могут быть повреждены, утрачены или украдены.

Чем больше используются ресурсы информационной системы, тем более уязвимой она становится. В системе может возникнуть поддельная электронная корреспонденция, конфиденциальная информация может быть опубликована в СМИ, конкуренты могут выявить информацию о ноу-хау организации — список угроз можно продолжать до бесконечности.

Угрозы, связанные с персоналом, могут быть идентифицированы страховой компанией. Скажем, сотрудник может попасть под машину (страхование от несчастного случая), может случиться производственная травма (страхование от несчастного случая на производстве) либо конкуренты решат переманить его более высокой зарплатой.

Что является объектом риска? У каждого объекта (ресурса) информационной системы есть стоимость. Для систематизации оценки стоимости ресурсов следует выделить следующие категории ресурсов:

Макрообъекты. Здания, в которых расположены объекты информационной системы, а также системы кондиционирования, другое поддерживающее оборудование. Макробъекты подвержены в основном рискам форс-мажорных обстоятельств, таких как пожар или наводнение, землетрясение или химическое заражение. Стоимость подобных ресурсов определяется исходя из затрат на запуск объектов информационной системы «с нуля» либо из затрат на их переустановку или восстановление.

Оборудование. Аппаратное обеспечение информационной системы, расположенное в рассматриваемой зоне, которое может выйти из строя. Сюда не включаются объекты, такие как канальное оборудование или АТС, расположенные вне макрообъектов организации. Стоимость данных ресурсов определяется как стоимость покупки оборудования с учетом амортизации плюс стоимость расходов на поддержку согласно договорам технической поддержки.

Программное обеспечение. Все программные продукты и документация, которые могут быть утрачены в случае разрушения информационной системы. В эту категорию входят как коммерческие программы (их стоимость определяется как цена покупки лицензии), так и программы собственной разработки (их стоимость оценивается как затраты на восстановление программного продукта с учетом того, что исходные коды и документация полностью утрачены).

Носители информации. Носители, которые будут утрачены при полном разрушении информационной системы. Их стоимость принимается равной затратам на закупку новых носителей.

Данные. Типовые методики количественной оценки стоимости информации фактически отсутствуют. Рекомендуется выделить ту информацию, которая является жизненно необходимой для функционирования организации (стратегические планы или операционные регламенты, бизнес-процессы, корпоративные базы данных, информация о

сотрудниках организации и т. д.) В данный список также может быть включена интеллектуальная собственность организации в случае, если рассматривается риск компрометации соответствующих данных (действительно, некоторые виды информации, например, ноу-хау, теряют свою стоимость по мере расширения круга лиц, ознакомленных с ними). Стоимость данных состоит из стоимости производства измерений, сбора данных и стоимости занесения данных на носитель.

Материалы. Стоимость вещественных активов, контролируемых либо учитываемых компьютерами, что делает возможным вмешательство в информационную систему с целью искажения информации о них.

Операции. Стоимость операционного бюджета всех действий, для которых необходимо использование компьютера.

Персонал. Зарплата сотрудников, участвующих в обслуживании информационной системы, а также в операционной деятельности.

Репутация фирмы. Несмотря на свою неочевидность, один из самых крупных и дорогостоящих информационных ресурсов. К примеру, при попытке получить крупный кредит утечка соответствующей информации может повлиять на решение банка.

Рассмотрим реальные угрозы безопасности системы:

Человеческий фактор. Системы проектируются и создаются людьми. Их развитие и наполнение также осуществляют люди. Человек склонен совершать ошибки, причем уровень критичности ошибок напрямую зависит от привилегий в системе. Частота (вероятность) совершения ошибки обратно пропорциональна уровню квалификации персонала, однако с ростом профессионализма персонала неизбежно растет фактор меры уязвимости ресурса к угрозе. Другими словами, более профессиональный работник может реализовать больший круг угроз, чем пользователь, обученный работе с системой строго в рамках выполнения поставленных ему задач.

Мошенничество и кражи. Информационные технологии все шире используются для совершения различных мошеннических действий. Компьютерные системы весьма **уязвимы как для традиционных, так и для новых методов мошенничества**. Финансовые системы не являются исключительным объектом для мошенников. Мошенничеству могут быть подвержены также системы контроля и учета рабочего времени, инвентарные системы, системы оценки труда, биллинговые системы. Бывшие сотрудники организации также являются источником угроз, особенно если их доступ не был соответствующим образом ограничен после увольнения.

Хакеры. Объектом атак со стороны хакеров являются не только вычислительные комплексы, базы данных, хранилища и центры обработки данных, но и активное сетевое оборудование, вмешательство в работу

которого зачастую имеет еще более плачевные последствия. Так, информация, циркулирующая через маршрутизатор, может быть перенаправлена по ложному адресу. Например, при компрометации учетных данных администратора и возможности удаленного доступа злоумышленник может изменить конфигурацию активного сетевого оборудования. При этом данное нарушение можно выявить только в случае установления контроля за целостностью конфигурации маршрутизатора, что на практике происходит достаточно редко. **Часто угрозе хакеров уделяется гораздо большее внимание, чем всем прочим угрозам.** Действительно, воздействие хакеров на информационные системы — достаточно распространенное явление. Кроме того, у организации есть возможность повлиять на внутреннего нарушителя административными мерами, однако нет такой возможности в отношении внешнего нарушителя — разве что в случае прямого нарушения уголовного или административного законодательства. Вместе с тем хакеры заставляют пользователей чувствовать себя уязвимыми, ведь фактически злоумышленник не определен. Наконец, организациям не известны истинные цели хакера; взлом системы может быть произведен с целью организации утечки, а может быть, и из спортивного интереса. Все эти допущения приводят к тому, что из всех возможных моделей хакера выбирается модель, способная реализовать наихудшие угрозы для информационной системы и нанести максимальный ущерб.

Промышленный шпионаж. Сбор информации об организации может осуществляться с целью ее передачи другой организации, которая в состоянии извлечь из этого для себя выгоду. К информации, утечка которой наносит максимальный ущерб, относится д**окументация о разработках, инженерная документация, данные о продажах, списки клиентов, сведения о разработках и планировании** и т. п.

Вредоносный код. Зачастую деятельность вредоносного кода (вирусы, «троянские кони», черви, «логические бомбы», прочие несанкционированные программы) ограничивают только сферой рабочих станций, однако она нередко распространяется и на куда более сложные системы. Выраженный в деньгах ущерб можно оценить, просуммировав потери от простоя системы и затраты на удаление вредоносного кода.

Угрозы персональным данным. Накопление большого количества персональных данных в информационных системах правительственных, финансовых и прочих организаций ведет к повышению интереса к подобным системам со стороны мошенников. Ввиду возможности агрегации, перезаписи, мониторинга и обработки подобных данных, возникает вполне реальная угроза персональным данным. Несанкционированная разведка персональных данных и их перепродажа заинтересованным лицам или организациям во многих странах признана незаконной. Такими данными может быть, например, **информация о**

годовом доходе, кредитная история, родственные связи, состояние банковских счетов, номера кредитных карт.

Есть и другие факторы, которые сложнее оценить, но, тем не менее, требуется принять во внимание: внутренние проблемы организации (например, факты нарушения трудового законодательства); стоимость утраты конфиденциальности информации; убытки при возможных судебных разбирательствах; стоимость утраты доступности информации.

Количественный и качественный анализ. Практика показывает, что самой большой проблемой в оценке рисков является оценка вероятности реализации той или иной угрозы. Наиболее часто вероятность реализации угрозы принимается исходя из наихудшего сценария развития событий. Другими словами, предполагается, что если угроза есть, то она будет реализована с вероятностью 100%. Тем самым параметр вероятности реализации угрозы фактически исключается из анализа и оценки рисков. Данный метод сложно назвать точным, так как его реализация на практике может повлечь избыточные расходы на средства защиты информации и, как следствие, повлечь нарушение принципа разумной достаточности затрат, в соответствии с которым стоимость средств защиты не должна превышать стоимость ресурса. Для точной оценки вероятности реализации угрозы целесообразно рассмотреть три величины:

- минимальная вероятность (например, при установке молниеотвода вероятность повреждения оборудования в результате попадания молнии составляет 0,0001%) — «оптимистичный прогноз»);
- наиболее вероятная оценка;
- максимальная вероятность (к примеру, в отсутствие молниеотвода вероятность повреждения оборудования в результате попадания молнии составляет 80%) —«пессимистичный прогноз»).

Принятие «оптимистичного» и «пессимистичного» прогнозов равными нулю и единице соответственно ведет к тому, что в **оценку рисков закладывается наиболее вероятная оценка реализации угрозы**, которая, однако, не равняется требуемой средней оценке вероятности реализации угрозы.

Можно попробовать вычислить оценку вероятности, однако разумнее всего просто обратиться к статистическим данным о прецедентах с подобными системами и получить достоверную информацию о стоимости ресурса, а также статистические данные о реализации угроз по отношению к этому ресурсу. В частности, подобным образом поступают страховые компании, принимая риски из прецедентных случаев вместо повторного расчета.

Так до 70% организаций имеют место инциденты с нарушением безопасности. Больше половины организаций (56%) понесли операционные убытки, 25% заявили о финансовых, а 12% — о других

видах убытков. В среднем на каждую организацию пришлось примерно 136 преступлений в сфере ИТ, тем не менее 30% организаций сообщили, что в их организациях подобных случаев не было, а 32% просто не подсчитывали понесенные убытки.

Направления защиты информации

Управление рисками необходимо для того, чтобы обеспечить возможность использования внутренних приложений, сведения к минимуму угрозы вторжения злоумышленника и раскрытия конфиденциальных данных. После идентификации угроз и рисков, направленных на системы требуется рассмотреть контрмеры. **Выбор контрмер должен производиться исходя из принципа разумной достаточности, то есть стоимость реализации контрмеры не должна превышать количественную величину убытков**. Таким образом, после идентификации контрмер требуется принять решение о действии над риском: предотвратить его, ограничить или принять (то есть не предпринимать никаких мер для снижения величины риска). Система защиты должна обеспечивать следующие характеристики информации:

- **конфиденциальность** – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации;

- **целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;

- **аутентичность** – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории называется фальсификацией автора сообщения;

- **апеллируемость** – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора третье лицо пытается заявить, что оно - автор сообщения, а при нарушении апеллируемости – сам автор пытается отказаться от своего авторства.

Основными принципами построения системы защиты являются:

- применение комбинированных аппаратно-программных средств;

- использование криптографических средств, имеющих соответствующие сертификаты.

При организации защиты любой системы необходимо иметь в виду следующие важные моменты.

Что дороже: предотвратить возможный ущерб, ограничить его или ничего предпринимать? Что тормозит построение комплексных систем информационной безопасности? Чтобы ответить на этот вопрос, следует оценить объекты угроз, связанные с ними риски, а также степень целесообразности защиты различных объектов в вашей организации.

Создание комплексных систем безопасности — обязательный сопутствующий фактор при реализации информационных систем любой сложности. Однако при создании системы информационной безопасности неизменно встает вопрос о целесообразности затрат на предлагаемые контрмеры. Ввиду отсутствия четких методик обоснования затрат процесс формирования системы информационной безопасности тормозится до принятия руководством организации решения о целесообразности (или нецелесообразности) подобных затрат.

Каждая угроза имеет вероятность ее проявления в рассматриваемой организации. Каждая угроза может иметь определенные *убытки от ее реализации за период в один год*. При этом следует принимать во внимание ряд моментов. При случайных реализациях угроз (например, при операционных ошибках или ошибках программирования) убытки зависят от времени простоя системы. При реализации угроз природного характера убытков рассчитывается исходя из нанесенного имущественного ущерба и времени простоя. При реализации угроз промышленного характера (например, выход из строя оборудования) убытки основывается на приблизительной стоимости запуска системы и стоимости времени простоя системы.

Как уменьшить риски? Свести величины рисков информационной системы к нулю невозможно. Поэтому, **действия по снижению риска должны быть в первую очередь направлены не на полное удаление риска, а на выбор эффективного метода управления данным риском и снижения риска до приемлемого уровня**. Рассмотрим некоторые типовые контрмеры.

Макрообъекты — самый распространенный объект управления рисками в страховых компаниях. В данном случае свои усилия следует направить на предотвращение возникновения последствий при стихийных бедствиях и природных явлениях — например, обеспечить грозозащиту, установить молниеотводы, источники бесперебойного питания, организовать систему пожаротушения и осуществить страхование в необходимом объеме.

Для предотвращения проблем с перебоями в электропитании требуется использовать источники бесперебойного питания. Также контрмеры в отношении оборудования могут включать применение систем кондиционирования (в том числе резервные системы кондиционирования), резервные серверы, узлы горячей замены, запчасти, инструментарий для проведения оперативного ремонта, заслоны для оборудования в случае

проникновения влаги в помещение. Фактическим стандартом является создание резервных центров обработки данных. Так, в документах из разряда описаний «лучших практик» заявляется, что основной и резервный центры должны быть разнесены на расстояние не менее 80 км, за счет этого достигается катастрофоустойчивость решения.

В отношении программного обеспечения основная контрмера — это, конечно же, создание резервных копий. Необходимо предусмотреть сохранение оригинальных дистрибутивов на отчуждаемом носителе. На случай утраты (выхода из строя) оригинального носителя требуется заключить с производителем коммерческого программного обеспечения соглашение о замене носителя. Сами носители целесообразно хранить в несгораемых шкафах на отдельном макрообъекте.

На случай выхода из строя информационной системы должна быть предусмотрена возможность продолжения работы с материалами на время восстановления информационной системы. Таким образом, нельзя полностью отказываться от использования «бумажного» документооборота, дабы при внезапном выходе информационной системы из строя была возможность продолжить работу в аварийном режиме с использованием обычных средств документооборота.

Лица, от которых зависит функционирование информационной системы, должны иметь возможность в приемлемое время прибыть к объекту информационной системы с целью предотвращения дальнейшего развития инцидента, вне зависимости от характера инцидента. Так, в договоре с охранным агентством должно быть указано время, в течение которого его сотрудники при получении сигнала тревоги должны прибыть на объект. Кроме этого, требуется таким образом регламентировать действия в случае нештатных ситуаций, чтобы сотрудники, в чью непосредственную компетенцию не входят операции по восстановлению работоспособности системы, могли бы, руководствуясь регламентом, приостановить развитие инцидента или локализовать его причину. Данные регламенты являются подлежащими документами для основного документа, описывающего политику действий в нештатных ситуациях. Подобный документ (План действий в чрезвычайных ситуациях) содержит перечень ответственных лиц с их координатами и перечень соответствующих регламентов.

Критерии принятия риска. Не всеми рисками можно управлять с помощью методологии снижения значений рисков. Для каждой угрозы существует определенное количественное значение стоимости контрмеры, после которой риск реализации данной угрозы рекомендуется принять. Кроме того, есть существенная разница между процессом принятия риска и процессом его избегания (т. е. построения системы таким образом, чтобы идентифицированный риск в ней отсутствовал). Подход принятия риска реализует большую гибкость в построении системы, нежели подход

избегания риска, так как во втором случае система изначально строится по конфигурациям, которые не обязательно оптимальны для выполнения бизнес-операций. В методологии управления рисками подмену понятия принятия риска понятием избегания риска называют «иррациональным пессимизмом».

Процесс принятия рисков обязательно должен базироваться на реалистичных прогнозах относительно угроз. В основе данного процесса могут лежать следующие методики.

Оценка фактора соотношения стоимость/эффективность: если стоимость реализации описанных контрмер (включая передачу риска страховой компании) превышает стоимость самого ресурса или стоимость восстановления ресурса после применения к нему наиболее худшего сценария развития событий, то риск следует принять. В данном случае «худший» сценарий развития событий может включать вариант, при котором ресурс не подлежит восстановлению и потому требуется его полная замена.

Простое принятие риска подразумевает принятие риска в том случае, когда количественная оценка риска невозможна либо (другой крайний случай) она очевидна. Нет смысла производить длительные расчеты, достаточно просто принять данный риск.

Область информационной безопасности не подвержена невозможным или неизбежным катастрофам и бедствиям, против которых менеджеры по информационной безопасности беспомощны. Основной принцип — идентифицировать, оценить и минимизировать неопределенные (случайные) события, которые могут повлиять на ресурсы. На это нужны определенные силы и время, но сама работа вполне осуществима.

После того как перечень возможных рисков составлен, необходимо предпринять шаги к устранению уязвимых мест и разработке контрмер на случай атак. Применяемые для этой цели инструменты будут эффективными только в том случае, если все программное обеспечение в системе актуально (то есть используются текущие версии) и установлены все необходимые заплаты. Если вы внимательно подошли к вопросу идентификации компонентов системы, то у вас уже есть общее представление о том, какие именно заплаты нужны. Установив их, займитесь реализацией системы управления изменениями в программном обеспечении и данных. Эта система станет дополнительным источником сведений в том случае, если какому-то злоумышленнику удастся преодолеть выстроенные вами защитные бастионы.

Компетентные хакеры в большинстве случаев добиваются своего и в преступных целях устанавливают контроль над сетевым оборудованием, если им удается получить доступ к нему через IP. Администратор вынужден удовлетворить чрезвычайно противоречивые требования: с

одной стороны, эффективно осуществлять управление сетью, с другой — защищать ее. В крупных сетях названные проблемы решаются хотя бы частично, но небольшие и средние сети нередко подвергаются весьма реальной угрозе. В качестве возможного решения специалисты советуют использовать третью версию протокола SNMP, где предусмотрен ряд защитных механизмов.

Альтернативой могут служить виртуальные частные сети **Virtual Private Network (VPN).** Создание каналов, защищенных с помощью криптографических методов, также можно отнести к этому типу инструментов защиты, поскольку они обеспечивают разграничение доступа между корпоративной и открытой сетями. Очень часто решения для создания защищенных каналов интегрируются в сетевые экраны. Однако, в нашей стране ситуация с криптографическими средствами защиты еще неясна: легально разрешено использовать ограниченный круг алгоритмов, куда не включены зарубежные стандарты. Современные VPN-решения не зависят от используемого типа шифрования, поскольку могут интегрировать в себя внешние библиотеки. Использование сети с сервером терминалов, где передача осуществляется через порты консоли, также позволяет организовать управление вне основной сети и отделить пользователей от информации системы управления сетью. С помощью соответствующей системы обнаружения несанкционированного доступа достигается и значительное усовершенствование системы безопасности.

Надо иметь в виду при организации систем защиты данных, что **сами по себе технологические решения вас не спасут**. Даже самые лучшие продукты служат лишь для проведения в жизнь тех правил и процедур, которые устанавливаются и поддерживаются системными администраторами и играют решающую роль в организации защиты любого ИТ-ресурса. Большую часть времени и сил администраторы систем защиты тратят именно на разработку, реализацию и внедрение соответствующих правил и процедур.

При организации защиты информационных систем госучреждений эти правила и процедуры должны строго соответствовать четко определенному списку нормативных актов и законов.

Должна существовать "пирамида безопасности". На **рис**.1 показаны элементы, необходимые для создания безопасной информационной среды. Элементы, необходимые для создания безопасной информационной среды:

- **Политика и процедуры**, определяющие стандарты и методы управления безопасностью;
- **Строгая аутентификация** для управления доступом и обеспечения невозможности "бесследности" действий пользователя;
- **Авторизация**, разрешающая опознанному пользователю доступ в соответствующие области;

- **Шифрование** - обеспечивающее конфиденциальность информации;
- **Аудит** подтверждает эффективность процесса.

Рис.1 Элементы безопасности информационной системы

Каждый последующий уровень пирамиды зависит от предыдущего. Если хотя бы одно из требований, предъявляемых к элементам, не выполнено на более низком уровня, это не будет выполнено и на более верхнем.

Основными принципами безопасности являются:

- **Конфиденциальность** – предотвращение раскрытия информации неуполномоченным лицам.
- **Целостность** – предотвращение повреждения, искажения или изменения информации или служб.
- **Проверка подлинности (аутентификация)** – удостоверение личности или иного объекта перед предоставлением этой личности или объекту доступа к данным.
- **Проверка полномочий (авторизация)** – обеспечение доступа к данным только тем лицам, которые были надлежащим образом авторизованы и получили соответствующие права.
- **Доступность** – обеспечение работоспособности и доступности информационных ресурсов, служб и оборудования.
- **Доказательство причастности** – установление связи между пользователем или объектом и действием. Это необходимо для того, чтобы доказать связь определенного действия с подозреваемым, отрицающим свою причастность.

Решите, что вы намерены делать, чтобы управлять рисками. Направления и средства защиты представлены в табл.2.

Таблица 2

Направления и средства защиты

Направление защиты	Средство защиты
Контроль за доступом из Интернет, предотвращение взлома извне	Использование внутренних IP-адресов и маршрутизации; Применение межсетевого экрана Cisco PIX Firewall; Хранение общедоступных ресурсов на публичном Интернет- портале, создание демилитаризованной зоны.
Авторизация и идентификация абонентов, разграничение доступа к внутренней информации	Использование персональных аппаратных ключей на порт USB (токенов) с хранением ключей в энергонезависимой памяти; Индивидуальный пароль абонента с контролем периодичности его смены и попыток подбора; Синхронизация учетной информации и паролей информационных систем всех уровней; Многоуровневая система разграничения доступа (на уровне хранения данных – SQL Server и уровне приложений – Интранет и персонализируемые порталы); Обратный дозвон (call back) для коммутируемых линий.
Контроль за выходом абонентов в Интернет, ограничение выхода	Сервер полномочий и кэширования (MS Proxy Server); система анализа и ограничения трафика.
Закрытие сообщений	Использование унифицированных средств шифрации и аутентификации, имеющих необходимые российские сертификаты; шифрация сообщений электронной почты и электронная подпись; HTTPS-шифрация трафика.
Использование средств сервера данных	Сервер данных включает комплексную многоуровневую систему защиты от различных угроз (внешнее вторжение и атаки, перехват трафика, внутренние нарушения и ошибки персонала).
Проверка системы специальными средствами анализа	Можно ничего не проверять и ждать пока взломают вашу систему и надеяться, что ваша защита выдержит атаку, а можно ещё на этапе разработки защиты воспользовавшись инструментом анализа уязвимых мест. Инструмент анализа делает это всё автоматически, он имеет возможность пополнения своей базы новыми записями о "дырах" в безопасности, и он проверит, имеется

Направление защиты	Средство защиты
	ли какая-либо "дыра" в вашей системе. Анализ уязвимости может проводить как администратор безопасности, так и злоумышленник, готовя удалённое вторжение в систему. В отчёте имеется информация, что в данном месте возможна атака, даже выдаётся информация, как её предотвратить, но не говорится, как конкретно эта атака проводится.

Стратегические мероприятия:

- Пригласите на работу ведущих экспертов по безопасности.
- Обеспечьте использование в организации самых передовых технологий и активный поиск слабых мест в системе безопасности, непрерывно работая над тем, чтоб опережать злоумышленников независимо от применяемых технологий.
- Предложите непрерывное повышение квалификации сотрудникам, чтобы обеспечить первоочередной учет факторов безопасности.

Тактические действия:

- Убедитесь в том, что все имеющиеся приложения безопасны, проведя анализ относительного риска, связанного с каждым приложением.
- Требуйте оценки для всех приложений – имеющихся, обновляемых или вновь создаваемых.
- Обеспечьте учет всех исполнимых модулей во всех приложениях, разрабатываемых в организациях.
- Убедитесь в том, что во всех группах разработки приложений на протяжении всего цикла разработки, эксплуатации и обслуживания вопросы безопасности всегда стоят на первом месте.

Оперативные действия:

- Отслеживайте все текущие и планирующиеся выпуски приложений.
- Определяйте и классифицируйте уязвимые места системы безопасности.
- Создайте правила оценки риска, чтобы определить какие приложения требуют более тщательной проверки (например, приложения имеющие выход в Internet)
- Создайте и поддерживайте политику и инструкции, чтобы при проектировании группы разработки приложений могли выполнять тестирование на наличие уязвимых мест.

- Определите процедуры, гарантирующее выполнение процесса необходимых проверок безопасности для всех новых и очередных выпусков имеющихся приложений, а так же устранение всех проблем до окончательного выпуска.
- Установите экстренные процедуры для управления исключительными ситуациями.
- Требуйте, чтобы все сотрудники прошли обучение по безопасности, соответствующие занимаемой должности, и обеспечьте возможность для постоянного повышения квалификации.

Документируйте все, что вы делаете. Документация — это основа для эффективного и систематического проведения в жизнь плана защиты. В ней должны быть отражены следующие ключевые моменты.

В первую очередь, должна быть подробно документирована существующая конфигурация системы. Многие атаки строятся на скрытом внесении изменений в конфигурацию приложений или операционной системы. Четкая процедура регистрации в документации изменений при авторизованных модификациях системы окажет существенную помощь в обнаружении таких атак и устранении их последствий.

Многим государственным организациям ведение документации необходимо также для того, чтобы получить сертификаты, обязательные для государственных систем и систем, которые подключаются к государственным системам. В таких случаях документация должна соответствовать стандартам, установленным государством.

В документации подробно описываются информационные системы — имеющиеся активы, уязвимые места, возможные риски — и перечисляются меры, которые нужно предпринять в случае атаки. В ней также должен быть отражен процесс защиты, дана оценка системы защиты и процедуры постоянной оценки надежности защиты и установки обновлений. Крайне важно, чтобы по мере совершенствования информационных систем соответствующие дополнения вносились в документацию, только в этом случае она в каждый момент времени будет отражать реальное положение вещей.

Анализируйте то, что вы делаете. Создание и воплощение в жизнь плана защиты информации — это колоссальная задача, которую нельзя рассматривать как одноразовое мероприятие. Недопустимо относиться к ней по принципу «сделано и забыто». Защита — это непрерывный процесс, который требует наличия серьезного набора правил и процедур для управления системой и регулярной его переоценки. Сертификация систем защиты требует документально оформленного набора процедур переоценки, при которых тестируются и проверяются все вновь обнаруженные уязвимые места.

Из соображений здравого смысла все изменения в системе (от заплат на отдельных рабочих станциях до переходов на новые серверные операционные системы) должны быть полностью документированы. Конечно, нелегко отслеживать все модификации, сделанные в крупной и сложной системе, но все же поддерживать этот процесс намного проще, чем наводить порядок после разрушительной атаки.

Не забудьте о физической защите. Если за системой никто не будет следить во время сеанса работы привилегированных пользователей, какой бы надежной ни была политика доступа на основе паролей, она окажется абсолютно бесполезной, если клавиатурой компьютера, на котором работает привилегированный пользователь, кто-то иной воспользуется для того, чтобы нанести ущерб системе. Элементы системы, обеспечивающие доступ к корневым каталогам или доступ в систему в качестве привилегированного пользователя, должны располагаться в помещении со строго контролируемым доступом.

Продумайте и организуйте процессы резервного копирования и восстановления данных. Как бы хорошо ни был продуман ваш план защиты, никогда нельзя быть уверенным в его неуязвимости. Убедитесь в том, что процедуры резервного копирования обеспечивают сохранение всех критически важных изменений в данных и всех транзакций, а также в том, что процесс восстановления сведет к минимуму последствия даже самых серьезных сбоев в системе.

Изучите своих пользователей. Ограничьте, если это возможно, доступ к системе со стороны компьютеров с конкретными, известными IP-адресами. Введите максимально строгие ограничения и надежные схемы аутентификации для пользователей, получающих доступ с удаленных машин. Проверьте, чтобы пользователям не было предоставлено больше прав, чем необходимо. Старайтесь не допускать «расползания прав», то есть, предоставляя пользователям дополнительные права, необходимые им для выполнения новых обязанностей, не забывайте ограничивать допуск к тем функциям, которые стали им не нужны.

Обучайте своих пользователей. Убедитесь в том, что каждому пользователю известны все процедуры защиты информации, и он понимает, как следует соблюдать правила, обеспечивающие безопасность системы. Разъясните каждому пользователю, каковы будут последствия несоблюдения этих правил и процедур как для него лично, так и для всей организации. Проследите за тем, чтобы каждый новый сотрудник компании прошел курс обучения, посвященный вопросам защиты информационных систем.

Учитесь сами. Вы должны знать о своих системах и их уязвимых местах не меньше, чем те, кто намерен атаковать их. Следите за тем, чтобы вовремя устанавливались новые версии и заплаты для приложений, операционных систем и встроенных программ. Вы должны знать, какие из

них следует устанавливать на ваши системы безотлагательно, а какие могут подождать до следующей крупной модернизации.

Чтобы установить слежку за корпоративной сетью, взломщику достаточно получить в свое распоряжение сетевой принтер, при посредничестве которого он сможет шпионить за всеми компьютерами в сети и целенаправленно искать «дыры» в системе безопасности. Система обнаружения несанкционированного доступа ничего не заметит, так как речь идет всего лишь о принтере и о совершенно обычном обмене данными по протоколу SNMP.

Оснащенные функциями SNMP системы управления сетью при каждом запросе одновременно передают открытым текстом пароль, который злоумышленникам, при желании, не составит труда прочесть. Это позволяет осуществить атаку на важнейшие системы передачи — не только на маршрутизаторы или коммутаторы, но и на сетевые принтеры. Опытные специалисты на это возразят, что данные протокола SNMP в коммутируемой сети не доступны пользовательским компьютерам. Однако посредством процесса ARP Cache Poisoning хакер может перехватывать информацию и в сетях с коммутаторами. Несмотря на это, управление сетью как фактор риска с далеко идущими последствиями для информационной безопасности по-прежнему недооценивается, хотя понимание проблем безопасности при управлении сетью постепенно растет.

Соблюдение конфиденциальности личной информации в Интернете становится все более и более важным вопросом для рядовых пользователей Сети. Им важно знать, как именно владелец того или иного Интернет - ресурса собирается использовать информацию, получаемую от них через Интернет. В некоторых случаях посетителям сайтов приходится целиком и полностью полагаться на порядочность владельца сайта. И в этом смысле вопрос доверия посетителя к сайту в целом становится ключевым. Приведем несколько простых рекомендаций, которые помогут добиться доверия посетителей к Интернет-ресурсу.

- Сообщите посетителям о том, как именно вы собираетесь использовать полученную от них информацию.
- В случае, если полученная от посетителей информация может быть передана третьей стороне, сообщите посетителям об этом.
- В случае, если вы запрашиваете e-mail адрес посетителей, сообщите им, с какой целью это делается.
- В случае, если фиксируется IP-адрес посетителей, сообщите им, с какой целью это делается.
- Сообщите посетителям, что вы не несете никакой ответственности за их информационную безопасность в случае посещения ими Интернет-ресурсов, на которые ссылается ваш сайт.

- Сообщите посетителям, с какой целью вы используете на сайте интерактивные формы, и как будет использована полученная при их помощи информация.
- В случае, если на сайте используются гостевая книга или форум, сообщите посетителям о том, что вся опубликованная ими в этих разделах информация, становится общедоступной.
- Сообщите посетителям о том, каким именно образом они смогут отказаться от почтовой рассылки вашего сайта.
- Сообщите посетителям о том, каким образом они могут связаться с вами для выяснения вопросов, касающихся конфиденциальности получаемой вами информации.

Можно привести следующие типы скрытых текстов:

- настоящие имена создателей документов и их сотрудников или соответствующие имена пользователей;
- данные о пользователях организационного характера;
- версия Word и формат документа;
- имя пути файла документа;
- информация об аппаратном обеспечении, на котором создавался документ;
- имена принтеров;
- заголовки сообщений электронной почты или информация о Web-сервере;
- текстовые фрагменты, удаленные из документа в некоторый момент до сохранения;
- текстовые фрагменты из других документов, не имеющих отношения к данному, попавшие в него из-за ошибок в Word.

Инструментарий для исключения скрытых текстов: Antiword (*www.winfield.demon.nl*) — свободно распространяемый инструментарий, который преобразует документ Word в плоский ASCII-текст; Catdoc (*www.45.free.net/~vitus/ice/catdoc*) — инструмент, во многом аналогичный первому, но дающий иногда несколько отличные от первого результаты (для просмотра документов Word, посылаемых коллегами, не обременяющими себя заботами о том, сможет ли адресат прочитать присланное, пользователи Unix применяют оба эти средства).

Аппаратное обеспечение безопасности

На этом уровне чаще всего обеспечивают безопасность данных от случайных сбоев. Примерами таких средств могут служить RAID-массивы (обеспечивают дублирование данных на нескольких носителях), WatchDog-

Таймеры (обеспечивают перезагрузку компьютера или других цифровых устройств без человека в случае зависания), ИБП (обеспечивают сохранность данных в случае отключения питания). Кроме средств защиты от сбоев, существуют устройства защиты от несанкционированного доступа к данным. Перечислим некоторые из них: биометрические датчики (позволяют провести идентификацию пользователя, используются не только для ограничения доступа в помещения, но и как средство аутентификации при использовании компьютеров и разных средств хранения информации), средства шифрования внедряемые в канал связи (например, существуют специальные сетевые платы, которые позволяют осуществлять шифрование на аппаратном уровне, недостатком таких устройств является невозможность их использования в сетях с обычным оборудованием), специальные средства шифрования данных при их сохранении на носители (например, существует устройство, включаемое между материнской картой и жестким диском, которое осуществляет шифрование данных при записи и восстановление данных при чтении, без такого устройства правильно прочитать данные невозможно).

Программно-аппаратная система на базе токенов (персональных аппаратных ключей) предназначено для обеспечения сохранности и целостности данных и пользовательских прав доступа в корпоративных информационных системах. В качестве ключа используется токен - полнофункциональный аналог смарткарты, выполненный в виде брелка. Он напрямую подключается к компьютеру через USB порт и не требует наличия дополнительных устройств (карт-ридеров и пр.). Главное назначение токена - аутентификация пользователя при доступе к защищенным ресурсам и безопасное хранение паролей входа в систему, ключей шифрования, цифровых сертификатов, любой другой секретной информации.

Управление цифровыми сертификатами. Система управления сертификатами обеспечивает целостную среду управления доступом к ресурсам и системам. Выдав сертификат нужному пользователю, администратор может гарантировать, что определенные данные ввести в базу может только авторизованный сотрудник.

Сетевые экраны. Продукты этого класса занимаются управлением сетевыми потоками, реализуя политику удаленного доступа к корпоративным ресурсам. При этом могут учитываться самые разнообразные параметры фильтрации: IP-адреса и порты, используемый тип сервиса и другие параметры. Классические сетевые экраны не контролировали данные, передаваемые с использованием протоколов, но современные продукты этого класса имеют формализованное описание протоколов и блокируют их некорректное использование. Впрочем, сетевые экраны начального уровня встроены и в современные операционные системы.

Если вовсе избежать катастроф невозможно, то **уменьшить риск потери данных** вполне по силам любой компании. Например, использовать кластерные системы. Кластеры можно создавать как на одной площадке, так и географически распределенные — в зависимости от особенностей бизнеса, размеров и финансовых возможностей компании. Расположение системы на локальном кластере вряд ли поможет при глобальной катастрофе, но для нормально текущей работы вполне может обеспечить минимальные простои приложений и баз данных, а также миграцию тех же приложений и баз данных в случае сбоя или плановых изменений. Плюсом здесь также является отсутствие единой точки отказа.

Если два кластерных узла расположить на разных площадках в одном городе и объединить их с помощью оптоволокна, то это вполне может защитить данные от локальных катастроф и обеспечить быстрое восстановление. Такая архитектура исключает необходимость репликации данных. Ее недостаток — требуются значительные затраты на построение инфраструктуры сетей хранения.

Для объединения кластерных узлов можно использовать сети IP. Это решение помимо защиты данных от катастроф имеет более низкую стоимость за счет экономии на оптоволоконных соединениях и отказа от инфраструктуры сетей хранения (вместо этого используется репликация). Плюсом является и отсутствие ограничений по расстоянию.

Разнесение элементов кластера по удаленным друг от друга районам требует значительных затрат на поддержание данных в актуальном состоянии. Информационные системы многих компаний сегодня должны находиться в работоспособном состоянии круглые сутки из-за того, что филиалы зачастую расположены в разных часовых поясах.

Основным недостатком традиционных методов переустановки операционной системы или восстановления ее из резервного образа, а также восстановления данных из резервной копии является большое количество ручной работы. Это увеличивает время простоя. Кроме того, нет никакой гарантии сохранения целостности и согласованности восстановленных данных. Можно создать клон основного программного обеспечения и всегда устанавливать его после аварийной ситуации.

Для ускорения аварийного восстановления рекомендуется, как можно чаще производить резервное копирование; осуществлять восстановление с логически подключенных устройств, а не через сеть; периодически удалять из системы неиспользуемые данные; чтобы не переустанавливать ОС, лучше применять решения для восстановления «с железа».

Необходимо добиться оптимального соотношения производительности, доступности (надежного хранения и отказоустойчивости) и совокупной стоимости владения при условии максимального соответствия требованиям заказчика (Рис.2). рассмотрим

способы повышения отказоустойчивости системы хранения в случае сбоев технического и логического характера. Реализация каждого из них по-своему влияет на производительность и стоимость всего центра, а также может повлечь за собой изменения в его структуре. Наилучшим способом обеспечения непрерывности бизнес-процессов и сохранения данных в таких ситуациях остается построение резервного центра.

Спектр методов повышения отказоустойчивости систем хранения широк: это и дублирование компонентов оборудования, и выбор дисков, и размещение данных с точки зрения файловой системы, и обеспечение надежности транспорта для передачи данных, и встроенные средства приложений.

Рис.2. Задача построения системы хранения данных

Как правило, сбои технического характера происходят из-за нарушения функционирования какого-либо компонента центра обработки данных. Несмотря на самое тщательное тестирование оборудования всегда есть вероятность выхода его из строя. Сбои логического характера случаются по причинам нарушения целостности информации вследствие ошибок системного программного обеспечения или из-за неправильных действий персонала.

Повышение отказоустойчивости дисковых массивов может быть достигнуто полным или частичным дублированием компонентов оборудования. За последнее время никаких революционных новаций в этой области не появилось, а само по себе дублирование компонентов применяется практически во всех типах оборудования ИТ. Естественно, подобные решения предлагают все производители дисковых массивов, однако полное дублирование (системы, где дублируются все компоненты) реализовано лишь в некоторых продуктах, поэтому к их выбору нужно подходить очень внимательно.

Отказоустойчивость транспорта можно повысить несколькими способами. Наиболее распространенный — построение двух полностью независимых транспортных контуров с коммутаторами, кабелями и независимым электрическим питанием. Другой способ заключается в установке коммутаторов, отказоустойчивость которых обеспечивается на уровне электрического оборудования (наличие двух внутренних шин для коммутации независимых модулей ввода/вывода, раздельные контуры электрического питания и проч.).Повышение отказоустойчивости транспорта влечет за собой заметный рост стоимости оборудования и обслуживания, а также дополнительные затраты на системы мониторинга и управления транспортом и, кроме того, потребность в высококвалифицированном персонале. Вместе с тем, меры по обеспечению отказоустойчивости практически не сказываются на общей производительности системы, а в случае использования коммутаторов директорского класса возможно даже ее улучшение.

Некоторые проблемы из-за сбоя оборудования могут быть решены на уровне операционной системы или специализированного программного обеспечения. **Программными» решениями повышения отказоустойчивости** часто пытаются заменить дорогостоящее аппаратное дублирование — в результате решение удается значительно удешевить, но снижается производительность, появляются скрытые затраты на администрирование и поддержку.

Протоколирование файловой системы позволяет обеспечить согласованность данных при сбоях в работе массива или каналов связи. Практически все файловые системы имеют эту функцию, однако в случае ее применения для повышения надежности производительность работы с самой файловой системой снижается. Для разных файловых систем и выполняемых задач потери производительности составляют в среднем 5—10%.

При другой трактовке — это средства приложений, которые умеют организовывать зеркалирование данных на разные носители (и внутри одного массива, и на разные дисковые массивы).

Повышение отказоустойчивости в большинстве случаев приводит не только к удорожанию системы, но и к усложнению процесса мониторинга и, как следствие, к более сложному распределению ресурсов и управлению ими. Эти факторы, в свою очередь, ведут к необходимости повышения квалификации обслуживающего персонала, внедрения специализированных программ, что неизбежно ведет к увеличению эксплуатационных затрат и стоимости владения.

Контролю доступа отводит лишь две роли: удерживать пользователей от безответственных действий и предохранять от них систему наблюдения. Мониторингом называется не техническое наблюдение за сетью, а постоянный контроль за работой конечных

пользователей. Для этого применяются специальные фильтры содержимого, системы обнаружения вторжений и превентивно работающие и записывающие все коммуникации на предприятии инструменты, которые в своих журнальных файлах сохраняют информацию обо всех действиях каждого пользователя в сети.

Программные средства обеспечения безопасности

Главным средством защиты информации от несанкционированного доступа является аутентификация пользователя с помощью пароля. Здесь с точки зрения безопасности надо отметить два пункта: надежные средства шифрования для хранения и передачи паролей и правильная организация работы с паролями (будет рассмотрена позже). Кроме защиты от непосредственного доступа через сервисы следует обеспечить защиту данных при передаче. Сюда включаются средства шифрования (они обеспечивают защиту от несанкционированного доступа) и средства проверки подлинности данных. Средства шифрования можно разделить на две группы: использование защищенного канала передачи и передача шифрованных данных при использовании открытого канала. Средства проверки подлинности включают в себя разнообразные контрольные суммы (они прежде всего обеспечивают защиту от аппаратных сбоев и помех, но не способны защитить информацию от злоумышленника) и средства работы с цифровой подписью.

Шифровать надо не то, что вы отправляете, а то, что храните. Несмотря на всю очевидность того, что данные, «неподвижно» лежащие в хранилищах, гораздо более уязвимы, нежели те, что передаются по каналам связи, основные усилия большинства компаний прикладываются к шифрованию последних. В результате взломов защиты за последний год было потеряно или испорчено больше данных, нежели при использовании лазеек в приложениях и сети. Шифрование должно стать первым приоритетом. Только 30% компаний шифруют хранящиеся у них данные, несмотря на то, что атаки учащаются. Если вы храните зашифрованные данные и потеряете цифровой ключ шифрования или пароль доступа, вы уже не сможете их прочесть. Необходима гарантия того, что процедуры резервного копирования и получения разрешения на доступ являлись составной частью стратегии шифрования, которая должна предполагать хранение ключей и паролей на определенных условиях у третьей стороны.

Некоторая информация требует дополнительной защиты при хранении (например, протоколы исследований или конфиденциальные записи о клиентах), другая — нет. Следует как можно чаще анализировать информацию и проводить классификацию своих данных по степени необходимой защиты, точно определять ресурсы, требующие шифрования.

Переход предприятия на распространение информационной продукции через Web сайт открывает новые способы доступа к информации и ведет к значительному повышению роли безопасности.

Важнейшее значение здесь имеет проблема авторизации. Прежние методы авторизации, например пароль, уже недостаточны из-за их уязвимости в связи с все более совершенствующимися способами несанкционированного доступа. Сегодня для защиты доступа к данным необходимы средства строгой авторизации пользователя, включающие не менее двух факторов идентификации личности. Элементы, необходимые для создания безопасной информационной среды:

- Политика и процедуры, определяющие стандарты и методы управления безопасностью.
- Строгая аутентификация для управления доступом и обеспечения невозможности "бесследности" действий пользователя.
- Авторизация, разрешающая опознанному пользователю доступ в соответствующие области.
- Шифрование конфиденциальной информации.
- Если хотя бы одно из требований, предъявляемых к элементам, не выполнено на более низком уровня, это не будет выполнено и на более верхнем. Например, отпечатки пальцев, диаграмма голоса или сканирование сетчатки можно украсть.

К сожалению, ни одно из этих средств не обеспечивает строгой авторизации пользователя, хотя перечисленные выше средства обеспечивают конфиденциальность (к примеру, Kerberos и SSL) или целостность (Цифровая подпись).

Цифровая подпись электронной почты. Добавление цифровой подписи к электронному письму гарантирует, что любые последующие изменения текста сообщения будут обнаружены. Цифровая подпись включают в себя три принципа защиты электронной почты:

- Целостность содержания: Microsoft Outlook и Outlook Express дают пользователям возможность подписывать письма с использованием личного ключа. При этом вместе с подписанным письмом пересылается сертификат отправителя и его открытый ключ. Настроив клиентскую программу электронной почты, пользователь сможет автоматически подписывать исходящие сообщения;
- Проверка: когда пользователь посылает электронную почту, которая подписана цифровой подписью, получатель может немедленно подтвердить личность отправителя с использованием открытого ключа;
- Защита от отказа: отправитель не сможет отрицать факта отправки данного письма.

Шифрование электронной почты. Шифрование гарантирует защиту содержимого сообщений корпоративной электронной почты. Зашифрованное и подписанное сообщение не может быть никем прочитано

до расшифровки. Чтобы зашифровать сообщение, отправитель должен иметь копию открытого ключа получателя. Зашифрованное сообщение может быть расшифровано и прочитано только владельцем соответствующего личного ключа.

Шифрование трафика. Использование средств шифрации делает возможным создание защищенных корпоративных Интранет-систем, в которых обеспечивается конфиденциальность и целостность информации, передаваемой между броузером и Web-сервером по открытым IP-сетям, а также аутентификация взаимодействующих сторон.

При работе с сетью для защиты информации часто используют средства управления трафиком, маршрутизацией и фаерволы. При правильном их использовании можно обеспечить надежную защиту данных не только от непосредственного доступа через сервисы, но и при их передаче (например ограничение доступа в подсеть через которую идет передача данных). Так же есть возможность использования фаерволов для защиты от атак типа “отказ в обслуживании” (по крайней мере, были примеры успешного применения фаерволов для защиты от таких атак). К специальным программным средствам для обеспечения безопасности стоит так же отнести средства поиска уязвимостей (сканеры портов, скриптов, средства эмуляции атак и тд). Кроме средств для защиты данных от злоумышленника, существуют средства для защиты от аппаратных сбоев, например специальные журналируемые файловые системы, которые способны обеспечить восстановление данных при ошибках записи и неправильном завершении работы ОС (примеры таких систем Windows – NTFS, Linux – Ext3FS и ReiserFS). Кроме специальных средств защиты программный уровень включает правильное конфигурирование системы, и создание и использование программного обеспечения, защищенного от ошибок (хотя бы от грубых). Большинство уязвимостей UNIX-систем связанно как раз с неправильным конфигурированием и использованием уязвимых версий программного обеспечения. Примеры распространенных ошибок при конфигурировании Unix-систем: неправильное конфигурирование доступа к proxy-серверу может превести к проникновению в подсеть, защищенную фаерволом; неправильное конфигугрирование ftp-сервера может привести к несанкционированному доступу к данным или даже атаке типа “отказ в обслуживании”; неправильное управление паролями и правами доступа к файлам может дать злоумышленнику полный контроль над системой и т.д.

Gmail (http://gmail.google.com/) первой среди всех почтовых служб в интернете приступила к "сквозной" пометке всей исходящей корреспонденции цифровой подписью, которая надёжно идентифицирует отправителя. Технология DomainKeys (http://antispam.yahoo.com/domainkeys) разработана компанией Yahoo. Технология работает как стандартная криптосистема. Владелец почтового сервиса (отправитель) генерирует пару криптоключей (публичный и

приватный). При этом допускается генерация нескольких криптопар. Публичный ключ публикуется в DNS, а приватный ключ используется на почтовых серверах для пометки всей исходящей корреспонденции. Другая сторона (получатель) извлекает из поля "From" имя домена и отправляет запрос к серверу DNS, чтобы получить публичный ключ для этого домена, после чего проверяет валидность подписи в заголовке почтового сообщения.

Если технология DomainKeys будет поддерживаться всеми почтовыми серверами в интернете, то станет невозможным подделка адресов электронной почты, которой часто пользуются спамеры. Если же спамеры сами начнут подписывать свои письма, то можно будет легко вычислить их почтовые серверы и поместить их в карантин. С другой стороны, никто не мешает спамерам регистрировать аккаунты на бесплатных почтовых серверах и рассылать с них подписанный цифровой подписью спам.

В принципе, систему для проверки подписей можно установить не только на почтовых серверах, но и на компьютерах каждого пользователя, чтобы стало возможным зашифровывать всё сообщение целиком и подписывать его личным ключом. Криптосистемы вроде PGP предусматривают, что каждый пользователь генерирует свою личную криптопару из публичного и приватного ключа, после чего его письма невозможно ни прочитать, ни изменить.

Intrusion Prevention System (IPS). Системы предотвращения вторжений появились как нечто среднее между межсетевыми экранами и средствами категории IDS (intervention detection system — «система обнаружения вторжений»). IPS считает опасным любое некорректное или просто необычное использование сетевых протоколов, в отличие от сетевых экранов контролируя как входящий, так и исходящий потоки пакетов. Иногда IPS нужно обучить работе в штатном режиме, поскольку в них используются технологии распознавания образов. Все отклонения от нормы IPS в дальнейшем блокирует. IPS предотвращают использование скрытых каналов, которые могут возникать при использовании редких возможностей сетевых протоколов. Такие инструменты часто объединяют с сетевыми экранами. В качестве примера можно привести модуль Application Intelligence для сетевого экрана компании CheckPoint Software.

Public Key Infrastructure (PKI). Инфраструктура открытых ключей используется для надежной аутентификации пользователей с помощью технологии открытых ключей. При этом пользователю выдается сертификат, позволяющий шифровать сообщения только его владельцу, а расшифровывать любому желающему. С помощью таких сертификатов происходит взаимная проверка подлинности, например, в протоколе SSL. Продукты для управления сертификатами можно использовать для универсального входа в систему, организации VPN (в том числе и по

технологии SSL) и для генерации электронных подписей под документами. В качестве примера можно привести удостоверяющий центр, встроенный непосредственно в ОС Windows.

Системы обновлений. Большинство внешних атак направлено против конкретных ошибок программного обеспечения, поэтому их своевременное исправление повышает защищенность всей информационной системы предприятия. Однако организовать оперативное и правильное исправление ошибок в большой корпоративной сети для всех используемых продуктов непросто. Для решения этой задачи и появились продукты, которые занимаются централизованным управлением процесса обновления программного обеспечения. Одним из примеров такой системы является инструментарий Software Update Services от Microsoft, но его можно использовать только для обновления Windows. Коммерческие сервисы подобного рода позволяют обновлять программные продукты разных производителей.

Фильтры. Все фильтры (спам-фильтры, фильтры для предотвращения утечки конфиденциальной информации, почтовые антивирусы и т.п.) проверяют потоки информации для поиска и удаления опасных вложений. Традиционно фильтруется электронная почта, но есть продукты и для Web, и для других технологий передачи данных. Фильтры могут либо настраиваться извне, либо обучаться на примере эталонной выборки. В качестве примера можно привести свободно распространяемый инструментарий SpamAssassin.

Средства виртуализации. Инструментальные средства для разделения одной физической среды на несколько логических предназначены не для обеспечения безопасности, однако, их можно учитывать в корпоративной политике безопасности как инструмент разграничения полномочий. Они могут использоваться для реализации на одном сервере нескольких различных политик безопасности для различных подразделений компании, например, при организации центра обработки данных и консолидации приложений. Виртуализация может осуществляться на уровне сети, операционной системы, приложений и подсистемы хранения данных.

У всех перечисленных классов программных продуктов есть и средства управления, и средства мониторинга, но все они относятся к типу исполнительных устройств, поскольку занимаются применением правил, заложенных в корпоративной политике безопасности, а также порождают поток событий, контролируемый системами мониторинга. Продуктов этого типа, работающих в самых разных уголках информационного пространства компании, в отличие от управления и мониторинга, может быть много. Это обеспечивает максимальный контроль со стороны ИТ-службы.

Управление идентификационной информацией. Любое средство управления идентификацией предназначено для того, чтобы в

информационной системе содержалась максимально подробная и актуальная информация о пользователях. В дальнейшем она используется всеми средствами разграничения доступа для оценки необходимости доступа конкретных пользователей к конкретным ресурсам, поскольку добавление новых пользователей или ролей через продукты этого класса приводит к появлению новых учетных записей и новых правил доступа для их использования.

Инструменты моделирования. Продукты этого класса (их еще называют системами управления рисками) позволяют проанализировать конфигурацию информационной системы, выделить требующие защиты ресурсы и с помощью моделирования найти конфигурацию защитных механизмов, которая бы оптимально защищала от наиболее опасных угроз, минимизируя потенциальные потери — риски. Некоторые системы этого класса по результатам моделирования могут выдавать конфигурационные файлы для защитных инструментов, таких, как межсетевые экраны.

Корреляционные системы. Эти продукты автоматизируют процессы изменения конфигурации исполнительных систем на основе данных, собранных механизмами мониторинга. Так достигается оперативное автоматическое переключение конфигураций защитных механизмов. Корреляционные системы ускоряют реакцию на атаку, а в отдельных простых случаях даже способны ее отразить.

Единая консоль управления. Обычно производители с большой продуктовой линейкой разрабатывают консоль для централизованного управления своими решениями. Но не все предприятия обходятся продуктами только одного производителя, поэтому зачастую для каждой группы защитных механизмов используется отдельная консоль, которая плохо координирует свои действия с решениями других производителей. Поэтому возник класс инструментов, позволяющих управлять защитой от разных производителей. Информацию они получают от средств обработки событий.

Детекторы вторжений собирают информацию о защищаемой системе и в случае возникновения подозрений поднимают тревогу. Контролироваться могут сетевые потоки и сообщения от сетевых экранов (сетевые детекторы), а также процессы ОС и открываемые порты (системные детекторы). Существуют также детекторы вторжений в базы данных и другие приложения. Традиционно подобные инструменты используют сигнатуры уже известных атак, но в последнее время наметилась тенденция применять в них методы систем категории IDP (гибридные средства обозначают термином Intrusion Detection and Prevention), которые используют технологии искусственного интеллекта.

Детекторы дефектов. Служба безопасности может не ждать атаки злонамеренных нападающих для проверки надежности своей защиты, а самостоятельно проводить их. Для этого можно использовать детекторы

дефектов или сканеры уязвимостей. Они автоматизируют проведение стандартных атак, не нанося вреда и проверяя реальный уровень защищенности корпоративной среды. Детекторы дефектов подготавливают списки уязвимых мест корпоративной системы и рекомендации по их защите. Эта информация в дальнейшем может быть использована для изменения политики безопасности предприятий.

Средства управления событиями. Корпоративная система ежесекундно порождает огромное количество событий, которые записываются в системные журналы. Часть из них имеет отношение и к событиям безопасности. Их нужно уметь выделить из общего потока и привлечь к ним внимание администраторов. Системы обработки событий предназначены, в основном, для административных нужд и учета ресурсов, однако, их можно использовать и для отправки оповещения сотрудникам службы безопасности о подозрительной активности. С помощью системы управления событиями можно автоматизировать реакцию системы на нападения, поскольку продукты этого класса, как правило, имеют возможность автоматического изменения конфигурации системы.

Системы предупреждения. Системы данного класса с помощью датчиков, расположенных в разнообразных частях Сети, контролируют общую активность пользователей Internet, пытаясь найти в ней подозрительную активность. Как только эксперты, контролирующие такую глобальную систему мониторинга, обнаруживают появление нового вируса или троянского коня, они рассылают предупреждения всем своим подписчикам с рекомендациями защиты от новой угрозы. Есть аналогичные глобальные системы мониторинга, которые следят за появлением новых сообщений о найденных ошибках.

Ловушки. Хорошим средством мониторинга нападений являются ловушки, которые специально предназначены для привлечения хакерской активности нападающих. Внешне ловушка выглядит как очень привлекательный ресурс, на котором происходит определенная активность. Однако это виртуальная среда, которая лишь создает видимость бурной деятельности, но основная ее задача как можно подробнее фиксировать действия посетителей. Легальные пользователи на нее не должны попадать, поэтому все заходящие по умолчанию считаются злоумышленниками и система должна собрать на них максимально подробное досье.

Помеха. Нападение, основная цель которого помешать служащим исполнению своих обязанностей, как правило, связано с передачей пользователю информации или программы, которую он не запрашивал. Для защиты от этого типа нападений логично использовать фильтрацию — спам-фильтр и антивирусы. Кроме того, если вирус направлен против конкретного дефекта в программном продукте нужно задействовать и систему обновлений. Избавление от этого типа нападений повышает

эффективность использования ресурсов, как вычислительных и сетевых, так и людских.

Утечка конфиденциальной информации. Предотвращение утечки — сложная задача, особенно если воруют информацию внутренние злоумышленники. Здесь могут пригодиться и решения VPN, и надежная идентификация PKI, и фильтрация по содержанию исходящего потока информации, и системы предотвращения вторжений IDP. Правда, ни одно из перечисленных средств не дает полной гарантии, что утечка не произойдет по не защищаемым им каналам, поэтому лучше максимально защитить все каналы или хотя бы контролировать передачу информации по ним.

DoS-атака. Атаки, направленные на отказ в обслуживании, часто связаны с какой-либо программной ошибкой, поэтому в большинстве случаев достаточно своевременно обновлять программное обеспечение. Более сложные распределенные DoS-атаки можно блокировать на уровне сетевого экрана или IDS/IPS. сейчас появляется новый класс продуктов для защиты от DoS-атак; в частности, один из них выпустила компания Cisco. Впрочем, для компаний лучше, если борьбой с DoS-атаками займется ее провайдер. В качестве примера можно привести компанию TeliaSonera и некоторых ее клиентов, которые выделяют DDoS-трафик и не учитывают его в расчетах со своими клиентами.

Захват. Традиционно для защиты от захвата используют сетевые экраны, IDS/IPS, системы идентификации и контроля доступа, но не стоит забывать о системах обновлений и об антивирусах. Для захвата используют самые изощренные методы нападения, поэтому для защиты стоит использовать несколько методов. Заниматься защитой от нападений нужно, поскольку это очень популярная цель индивидуальных атак, которые могут оказаться очень разрушительными.

Организационный уровень обеспечения безопасности

Большинство успешных атак в истории были реализованы благодаря человеческому фактору. Человек – самое уязвимое звено в системе безопасности. Рассмотрим основные направления организационной деятельности по обеспечению безопасности данных. Одна из наиболее распространенных причин успешности атак – выбор пользователями и системными администраторами слабых паролей (например, атака на слабые пароли было одним из основных средств проникновения вируса Морриса). К сожалению часто одних организационных мероприятий не достаточно. Если системных администраторов еще можно убедить выбирать пороли стойкие к подбору, то пользователи всегда будут выбирать слабые пароли. Эта проблема частично решается на программном уровне. Существуют средства препятствующие выбору слабых паролей. Здесь существуют три основных направления. Первое – проверка пароля при его установке (если почтовые службы проверяют

только размер пароля, то, например утилита passwd в Unix проверяет и сам пароль). Второе – использование генераторов паролей. При этом пользователь не сам выбирает пароль, а его случайным образом генерирует специальная программа. Третье – проверка паролей после установки путем подбора.

Кроме обеспечения стойкости паролей для сохранности информации необходимо провести работу с персоналом на предмет неразглашения конфиденциальной информации, исключения сохранения ее на ненадежные носители и перепроверке личности запросившей информацию. Часто злоумышленники для осуществления взлома используют телефон, выдают себя за системного администратора и получают данные необходимые для проникновения в систему. Другой пример, часто операторы компьютеро, когда не могут запомнить сложный пароль, записывают его на листке бумаги, который может попасть к злоумышленнику. Всех приведенных выше средств будет недостаточно чтобы обеспечить безопасность, если системный администратор будет игнорировать последние обновления ПО и выпуски бюллетеней, новостных лент, рассылок и тд., посвященных проблемам безопасности. Яркий пример – известная атака сетевого червя Slammer. Известно, что уязвимость в Windows, которую использовал червь, была обнаружена давно. Даже соответствующий патч от Microsoft был выпущен за несколько месяцев до атаки. Но большинство администраторов Windows2000 это проигнорировали, в результате чего большая часть Internet была парализована. Можно привести еще много примеров нарушения безопасности на организационном уровне, приведем пару из них. Часто фирмы и даже крупные корпорации продают устаревшие жесткие носители, которые раньше содержали секретную информацию, проведя при этом только “быстрое” форматирование или даже вообще без форматирования. Другой пример, некоторые системные администраторы часто оставляют терминалы с правами суперпользователя без присмотра.

Пароли пользователей. Важнейшее значение здесь имеет проблема авторизации. Прежние методы авторизации уже недостаточны из-за их уязвимости в связи с все более совершенствующимися способами несанкционированного доступа. Сегодня для защиты доступа к данным необходимы средства строгой авторизации пользователя, включающие не менее двух факторов идентификации личности. Средства персонализации помогают удерживать клиентов на Web сайте. Чтобы создать безопасные Web сайты и сети требуется организовать многоуровневый подход к защите информации. Усиленные средства аутентификации пользователя, в сочетании с другими технологиями, помогут обеспечить правильность учета пользователей, конфиденциальность работы и возможность полноценного аудита. Авторизация не может существовать сама по себе.

Есть множество программ, которые делают перебор паролей по словарю. Данная проверка должна исключать плохо выбранные пароли

пользователями. Следите за тем, чтобы они были достаточно длинными, нестандартными и регулярно менялись. **Пароли должны иметь в длину не меньше шести символов и представлять собой слова**, которые нельзя найти в словарях (они должны содержать как буквы, так и цифры). Заставляйте пользователей регулярно менять пароли. Все это, по-видимому, не вызовет у них особого энтузиазма, однако если не соблюдать эти требования, никто не сможет поручиться за надежность системы защиты. Билл Гейтс заявил, что пароли как средства обеспечения информационной безопасности обречены на вымирание, будущее за технологиями управления идентификацией, основанными на радиометках, биометрии, смарт-картах. Каждый сотрудник с помощью одной лишь карты сможет входить и выходить из здания, получать доступ к своей машине, они заменят все пароли.

Должна быть разработана специальная программа и правила, которые должен знать любой сотрудник, получающий доступ к ИТ-ресурсам компании в которой представлены описания политики защиты, правила безопасности. С этими правилами должны быть ознакомлены все сотрудники. Каждый новый сотрудник должен изучить правила соблюдения информационной безопасности и подписал документ, что с ними ознакомлен.

Необходимо создать Web-страницу, посвященную защите информации, где опубликовать правила информационной безопасности при работе в компании, процедуры и основные принципы.

Программа тренинга для новых сотрудников должна включать:

каждый сотрудник компании обязан периодически просматривать intranet в поисках новой информации, изучить правила и принципы организации защиты данных.

провести серию неформальных бесед и попросить отдел кадров разослать по электронной почте сообщения, подчеркивающие необходимость соблюдать и изучать правила безопасности.

поиск новых инструментов, которые помогут в распространении информации об этих правилах.

нужно Web-приложение, способное проверять, какие сотрудники изучили правила и прочитали ли они все сведения, которые касаются выполнения их служебных обязанностей.

Пароль, можно угадать, сообщить или забыть. Наиболее надежно "То, что Вам присуще", однако реализация этого принципа дорога, а результат недостаточно надежен. Использование двух типов авторизации развивает концепцию "небесследности" - Вы не только подтверждаете собственную личность и получаете доступ к ресурсам, но и впоследствии не сможете отрицать осуществление этого доступа. Пароли являются прекрасным примером того, насколько уязвимой может быть

однофакторная авторизация. Ранее большинство многопользовательских систем для управления доступом к процессорному времени и определению размеров оплаты для каждого из пользователей полагались исключительно на авторизацию по паролю. В настоящее время пароль нужен в основном для управления доступом к данным; почти во всех вариантах UNIX, Windows NT и других операционных средах система безопасности допускает повторное использование паролей. В зависимости от ценности защищаемой информации повторного пароля может быть достаточно, однако программы перехвата нажатий клавиш и сетевых становятся все более опасными для такого метода. В этом случае сообщения от одного компьютера другому попадают на все стоящие в сети, а обрабатываются только на том, для которого они собственно и предназначались. Однако любой компьютер в сети может начать чтение и запись всех приходящих сообщений, содержащих в том числе и пароли, а затем использовать собранные сообщения для несанкционированного доступа. Имеются (**Firewall) з**ащитные барьеры, отделяющие внутренние системы предприятия от внешней среды и фильтрующий нежелательные пакеты данных. Реализован в маршрутизаторе либо использует сочетание маршрутизаторов и рабочих станциях.

Важнейший фактор, влияющий на принятие решения о необходимости использования средств строгой авторизации, - это размер ущерба, причиняемый несанкционированным доступом к охраняемым данным. Может быть, и не стоит усложнять управление доступом к несекретным данным, однако доступ к конфиденциальной информации потребует гарантии ответственности пользователя, которую могут обеспечить только средства строгой авторизации.

Принципы разграничения прав в системе, основаны на использовании понятий профилей категорий пользователей и профилей категорий доступа. Доступ может определяться к каким – либо операциям в системе или к каким-нибудь элементам классификации ресурсов в системе : к элементу каталога в иерархической системе каталога или к каком-либо элементам описания ИР. Таким образом, объектом доступа могут быть операции, элементы каталога, элементы описания ИР. Каждой категории доступа ставится в соответствие правила доступа к объекту. Каждому объекту доступа может быть поставлен в соответствие собственный список категорий доступа (или одна категория), т. е. профиль объекта доступа. Категории пользователей – это те роли, которые могут возникать при взаимодействии пользователей с системой при решении тех или иных прикладных задач.

Каждой категории пользователей ставится в соответствие ее профиль путем перечисления привилегий - сочетания конкретной категории доступа с конкретным объектом доступа. Таким образом, определяются категории пользователей, определяются категории доступа, формируются профили для каждой категории пользователей, определяются профили для каждого

объекта доступа. При каждом обращении конкретного пользователя к некоторому объекту доступа происходит сверка профиля его пользовательской категории с профилем конкретного объекта доступа. Окончательный набор возможностей пользователя является пересечением обоих профилей. Этот способ является альтернативным способу разграничения прав на ресурсы (или каталоги). Единая система прав для доступа к операциям, ресурсам и описаниям ИР должна обладать гибкостью и настраиваемостью для конкретных задач.

Для реализации разграничения прав доступа к ресурсам при поиске по описаниям ИР можно использовать несколько путей:

-Использовать внешние механизмы для разграничения прав на конкретные ресурсы, например, отдельные таблицы доступа с соответствующими программными модулями фильтрации при поиске;

-Использовать специальный механизм поиска по рубрикаторам, в котором количество доступных пользователю элементов рубрикатора зависит от его уровня доступа;

-Включить информацию о доступе пользователей различных уровней в описание информационного ресурса.

Более трети проблем информационной безопасности связаны с действиями персонала. Сейчас около 90% информационных систем защищены простым паролем, который достаточно несложно перехватить или подобрать. К тому же пользователям трудно запоминать уникальные и сложные пароли, поэтому они начинают либо повторно применять пароли из других систем, либо записывать их. И то и другое не способствует надежности защиты. Для защиты от них можно воспользоваться технологиями проверки и хранения идентификационной информации.

Необходимо применять трехфакторную технологию идентификации пользователей: по USB-ключу, PIN-коду и отпечатку пальца. При извлечении ключа из разъема доступ ко всем связанным с ним приложениям блокируется.

В основе организационных мер защиты информации лежат **политики безопасности**. От их эффективности в наибольшей степени зависит успешность любых мероприятий по обеспечению информационной безопасности. Часто приходится сталкиваться с неоднозначностью понимания термина «политика безопасности». В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению информационной безопасности организации. В узком — как локальный нормативный документ, определяющий требования безопасности, систему мер либо порядок действий, а также ответственность сотрудников и механизмы контроля для определенной области обеспечения информационной безопасности. Примерами таких документов могут

служить «Политика управления паролями», «Политика управления доступом к ресурсам корпоративной сети», «Политика обеспечения информационной безопасности при взаимодействии с Internet» и т. п. Использование нескольких специализированных нормативных документов обычно предпочтительнее создания «Общего руководства по обеспечению информационной безопасности организации». Скажем, в компании Cisco Systems стараются, чтобы размер политики безопасности не превышал двух страниц; в редких случаях он может достигать четырех-пяти страниц. Этот подход, однако, не противоречит созданию объемных руководств, положений и концепций, содержащих ссылки на множество специализированных политик безопасности и увязывающих их в единую систему организационных мер по защите информации.

Рассмотрим существующие подходы к разработке эффективных политик безопасности, без которых невозможно создание комплексной системы информационной безопасности организации. Эффективность политики безопасности определяется качеством самого документа, который должен соответствовать текущему положению дел в организации и учитывать основные принципы обеспечения информационной безопасности, а также правильностью и законченностью процесса внедрения.

Политики безопасности терпят неудачу по целому ряду причин:

Политики безопасности были неудобны для сотрудников организации и оказывали негативное влияние на эффективность бизнес-процессов;

Сотрудники и менеджеры не привлекались к разработке политики безопасности, ее требования не согласовывались со всеми заинтересованными сторонами;

Сотрудники и руководство организации не были осведомлены о причинах, обусловливающих необходимость выполнения правил политики безопасности;

Контроль выполнения политики безопасности в ходе их внедрения не осуществлялся;

Аудит безопасности не проводился;

Правила политики безопасности не пересматривались.

Факторы, обусловливающие эффективность политики безопасности. Эффективные политики определяют необходимый и достаточный набор требований, позволяющих уменьшить риски информационной безопасности до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками.

Безопасность препятствует прогрессу. Меры безопасности накладывают ограничения на действия пользователей и системных администраторов и в общем случае приводят к снижению производительности труда. Безопасность — затратная статья, как и любая другая форма страхования рисков. Человеческая природа всегда порождает желание получить большее количество информации, упростить доступ к ней и уменьшить время реакции системы. Любые меры безопасности в определенной степени препятствуют этому. Каждый пользователь обладает ограниченным запасом терпения в отношении правил политики безопасности, достигнув предела которого он перестает им следовать, решив, что это явно не в его интересах (не в интересах дела). Политики, не учитывающие влияния, которое они оказывают на производительность труда пользователей и на бизнес-процессы, в лучшем случае могут привести к ложному чувству защищенности. В худшем случае такие политики создают дополнительные бреши в системе защиты, когда «кто-то начинает двигаться на красный свет». *Следует учитывать и минимизировать влияние политики безопасности на производственный процесс, соблюдая принцип разумной достаточности.*

Навыки безопасного поведения приобретаются в процессе обучения. Процедура обеспечения информационной безопасности требует обучения и периодического поддержания. Здесь нельзя полагаться на интуицию, необходимо осознавать ценность информационных ресурсов, риски и размеры возможного ущерба. Пользователь, не имеющий представления о критичности информационных ресурсов или о причинах, по которым их следует защищать, скорее всего, будет считать соответствующую политику неразумной. Руководство организации также следует просвещать по вопросам, касающимся ценности информационных ресурсов, ассоциированных с ними рисков и соответствующих политик безопасности. Если руководство не знакомо с политикой безопасности или с ее обоснованием, не приходится рассчитывать на его поддержку. Конечно, руководству не обязательно знать технические детали обеспечения информационной безопасности и конкретные правила, предписываемые политиками. Достаточно сфокусировать его внимание на возможных последствиях нарушений безопасности и связанных с ними потерях для организации.

Следует проводить непрерывную работу по обучению сотрудников и повышению осведомленности руководства организации в вопросах обеспечения информационной безопасности.

Необходимо осуществлять непрерывный контроль выполнения правил политики безопасности как на этапе ее внедрения, так и в дальнейшем, фиксировать нарушения, разбираться в их причинах. Одна из основных форм этого контроля — регулярное проведение как внутреннего, так и внешнего аудита безопасности.

Политику безопасности необходимо совершенствовать, чтобы она оставалась эффективной. Даже если вам удалось разработать и внедрить эффективную политику безопасности, работа на этом не заканчивается. Обеспечение информационной безопасности — непрерывный процесс. Технологии стремительно изменяются, системы устаревают, а многие процедуры теряют эффективность. Политики безопасности должны непрерывно совершенствоваться, чтобы оставаться эффективными. *Работоспособность и эффективность существующих политик должны регулярно проверяться. Устаревшие политики должны пересматриваться.*

Рекомендации по разработке и внедрению эффективных политик

Предприятия должны тестировать веб- приложения на предмет наличия дефектов безопасности с той же жесткостью, с какой они тестируют аппаратуру и сети. Более частое проведение тестов на взлом поможет снизить опасения потребителей. Чем чаще вы испытываете вашу систему, тем больше ваша уверенность в надежности используемых приложений. Эту уверенность можно и нужно донести до конечного потребителя.

Учет основных факторов, влияющих на эффективность политик безопасности, определяет успешность ее разработки и внедрения. Минимизация влияния политики безопасности на производственный процесс. Внедрение политики безопасности практически всегда связано с созданием некоторых неудобств для сотрудников организации и снижением производительности бизнес-процессов. В то же время не стоит стремиться сделать меры информационной безопасности абсолютно прозрачными. С целью понять, какое влияние политика будет оказывать на работу организации, и избежать узких мест следует привлекать к разработке этого документа представителей бизнес-подразделений, служб технической поддержки и всех, кого это непосредственно коснется. Политика безопасности — продукт коллективного творчества. В состав рабочей группы рекомендуется включить: руководителя высшего звена; руководителя, ответственного за внедрение и контроль выполнения требований политики безопасности; сотрудника юридического департамента; сотрудника службы персонала; представителя бизнес-пользователей; технического писателя; эксперта по разработке политики безопасности. В рабочую группу может входить от 5 до 10 человек в зависимости от размера организации и широты проблемной области, охватываемой политикой безопасности.

Обучение пользователей и системных администраторов — важнейшее условие успешного внедрения политики безопасности. Только сознательное выполнение ее требований приводит к положительному результату. Обучение реализуется путем ознакомления всех пользователей под роспись, публикации политики безопасности, рассылки пользователям

информационных писем, проведения семинаров, а также индивидуальной разъяснительной работы с нарушителями. В случае необходимости на нарушителей безопасности налагаются взыскания, предусмотренные политикой безопасности и правилами внутреннего распорядка. Пользователи должны знать, кого, в каких случаях и каким образом информировать о нарушениях информационной безопасности. Контактная информация лиц, отвечающих за реагирование на инциденты, должна быть доступна любому пользователю.

Контроль выполнения правил политики безопасности может осуществляться путем проведения плановых проверок в рамках мероприятий по аудиту информационной безопасности. В организации должны быть предусмотрены меры по реагированию на нарушение правил политики безопасности. К этим мерам относятся оповещение об инциденте, реагирование, процедуры восстановления, механизмы сбора доказательств, проведения расследования и привлечения нарушителя к ответственности. Система мер по реагированию на инциденты должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала. Необходимо, чтобы политики по возможности носили не рекомендательный, а обязательный характер, ответственность за их нарушение была четко определена, а также были предусмотрены конкретные дисциплинарные и административные взыскания.

Постоянное совершенствование политик безопасности. Политика безопасности — это не набор раз и навсегда определенных прописных истин. Не следует пытаться путем ее внедрения решить сразу все проблемы безопасности. Политика является результатом согласованных решений, определяющих основные требования по обеспечению информационной безопасности и отражающих существующий уровень понимания этой проблемы в организации. Для того чтобы оставаться эффективной, политика безопасности должна периодически корректироваться. Необходимо определить ответственность за поддержание политики безопасности в актуальном состоянии и назначить интервалы ее пересмотра. Политика должна быть простой и понятной. Следует избегать усложнений, которые сделают политику неработоспособной. По этой же причине описание политик не должно быть длинным. Иначе большинство пользователей не дочитают ее до конца, а если и дочитают, то не запомнят, о чем в ней говорится.

На этапе внедрения политики безопасности решающее значение имеет **поддержка руководства организации**. Политика безопасности вводится в действие приказом руководителя, и процесс ее внедрения находится под его контролем. В политике безопасности прослеживается озабоченность руководства вопросами обеспечения информационной безопасности. Координатору рабочей группы по разработке политики безопасности следует разъяснить руководству организации риски, возникающие в случае отсутствия такой политики, а предписываемые ею

меры экономически обосновать. Разработка политики безопасности — длительный и трудоемкий процесс, требующий профессионализма, отличного знания нормативной базы в области безопасности, да и писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение информационной безопасности. Эта ответственность обычно концентрируется на руководителе отдела информационной безопасности, директоре по безопасности, ИТ- директоре или на руководителе отдела внутреннего аудита; именно он координирует деятельность рабочей группы по разработке и внедрению политики безопасности на протяжении всего жизненного цикла, который состоит из пяти последовательных этапов.

Первоначальный аудит безопасности. Аудит безопасности — процесс, с которого начинаются любые планомерные действия по обеспечению информационной безопасности в организации. Он включает в себя проведение обследования, идентификацию угроз безопасности, ресурсов, нуждающихся в защите и оценку рисков. В ходе аудита производится анализ текущего состояния информационной безопасности, выявляются существующие уязвимости, наиболее критичные области функционирования и самые чувствительные к угрозам безопасности бизнес-процессы.

Разработка. Аудит безопасности позволяет собрать и обобщить сведения, необходимые для разработки политики безопасности. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению информационной безопасности в организации, позволяющих уменьшить риски до приемлемой величины, которые оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации. Разработка политики безопасности с нуля не всегда является хорошей идеей. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта к специфическим условиям своей организации. Этот путь позволяет сэкономить месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки политики безопасности.

Внедрение. С наибольшими трудностями приходится сталкиваться на этапе внедрения политики безопасности, которое, как правило, связано с необходимостью решения технических, организационных и дисциплинарных проблем. Часть пользователей могут сознательно либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-технических механизмов защиты информации, в той или иной степени неизбежно

ограничивающих их свободный доступ к информации. Системных администраторов может раздражать необходимость выполнения требований политик безопасности, усложняющих задачи администрирования. Помимо этого могут возникать и чисто технические проблемы, связанные, например, с отсутствием в используемых программных средствах функций, необходимых для реализации отдельных положений политики безопасности. На этапе внедрения необходимо не просто довести содержание политики до сведения всех сотрудников организации, но также обучить и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по-старому.

Аудит и контроль. Соблюдение положений политики безопасности обязательно для всех сотрудников организации и должно непрерывно контролироваться. Проведение планового аудита безопасности является одним из основных методов контроля работоспособности политики безопасности, позволяющего оценить эффективность внедрения. Результаты аудита могут служить основанием для пересмотра некоторых положений политики и внесения в них необходимых корректировок.

Пересмотр и корректировка. Первая версия политики безопасности обычно не в полной мере отвечает потребностям организации, однако понимание этого приходит с опытом. Скорее всего, после наблюдения за процессом внедрения и оценки эффективности ее применения потребуется осуществить ряд доработок. В дополнение к этому, используемые технологии и организация бизнес-процессов непрерывно изменяются, что приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности. Как правило, **ежегодный пересмотр политики безопасности** — норма, которая устанавливается самой политикой.

Адекватный уровень информационной безопасности в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных политик безопасности. Такие политики определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски информационной безопасности до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы политика безопасности оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах безопасности и обучать их выполнению правил, предписываемых ею. Регулярный пересмотр и корректировка правил политики безопасности необходимы для поддержания ее в актуальном состоянии.

Разработка и внедрение политики безопасности — процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство возлагает ответственность за обеспечение информационной безопасности. Этот специалист координирует деятельность рабочей группы по разработке и внедрению политики безопасности на протяжении всего жизненного цикла, включающего в себя проведение аудита безопасности, разработку, согласование, внедрение, обучение, контроль исполнения, пересмотр и корректировку политики безопасности.

Политики безопасности объединяются в **Методологию комплексного управления безопасностью** (КУБ), которая разграничивает полномочия каждого участника процесса. За бизнес- подразделением закрепляются вычислительные ресурсы, которыми оно может распоряжаться. Настройкой этих ресурсов, в соответствии с требованиями бизнеса, занимаются ИТ- службы. А сотрудники отдела безопасности контролируют правильность и санкционированность настроек.

В соответствии с этой моделью КУБ выполняет преобразование заявок в инструкции и мониторинг изменений конфигурационных файлов. Процесс работы с КУБом следующий: сотрудники бизнес- подразделений подают в КУБ заявки на доступ к тем или иным ресурсам, КУБ согласовывает все детали по заранее установленному регламенту и выдает инструкции для ИТ- специалистов по конфигурированию конкретных систем. Подробность инструкций можно варьировать в зависимости от требований заказчика и квалификации его ИТ- специалистов. После того как изменения внесены, КУБ фиксирует их и вместе со всей сопроводительной документацией передает сотрудникам информационной безопасности. Еще одной важной задачей КУБ является протоколирование всех действий всех подразделений, чтобы в дальнейшем можно было понять, с чем связаны те или иные ограничения безопасности и нельзя ли их снять.

С технической точки зрения КУБ представляет собой хранилище документов в формате XML с доступом к нему через Web-интерфейс и с оповещением по электронной почте. Кроме того, КУБ имеет агенты, которые собирают конфигурационную информацию с различных вычислительных ресурсов. Использование XML облегчает преобразование заявок, принятых через Web-интерфейс, в инструкции для администраторов. Второй компонент КУБ — средства контроля над изменениями конфигурационных файлов, который выполняется с помощью специальных агентов. Таким образом, чтобы осуществить администрирование любого нового ресурса, для него нужно составить правила преобразования запросов в инструкции и создать агенты для контроля над изменениями.

Сейчас эти компоненты реализованы для администрирования Windows. При этом контроль за изменениями ведется не только на уровне общей конфигурации операционной системы, но и с точностью до списков прав на доступ к отдельным файлам. Компания также реализовала универсальный агент, которому можно предписать наблюдение за конкретными файлами и запись всех обнаруженных изменений в хранилище КУБ.

Заключение

Число технологий защиты, предлагаемых на рынке, настолько велико, что знать все, пусть даже поверхностно, не под силу даже самым опытным ИТ- менеджерам. Для правильного выбора небесполезно иметь представление, какие из них могут вовсе не понадобиться. ИТ- менеджеры должны стараться заглянуть как можно дальше вперед, когда речь заходит о внедрении систем, и прежде всего добиваться их корректной работы, а не тратить время и деньги на исправление ошибок.

Программное обеспечение не должно иметь изъянов, и задача ИТ-менеджеров — стимулировать производителей к выпуску надежных программ, иначе расходы на защиту будут расти. Предприятия должны требовать подтверждения, что программы, которые они покупают, защищены, и производитель проанализировал код с учетом требований безопасности.

Несмотря на хорошую осведомленность руководителей компаний о рисках, которым подвергается информационная безопасность со стороны сотрудников их организаций, они не предпринимают адекватных мер. Организации по-прежнему уделяют основное внимание таким внешним угрозам, как вирусы, в то время как серьезность внутренних угроз постоянно недооценивается. Компании охотно идут на закупки технических средств, но не готовы относить кадровые проблемы к разряду приоритетных.

Разумеется, корпоративная сеть должна быть защищена по всему периметру, в целях безопасности произвести сегментирование сети, принять меры защиты информационных ресурсов, регулярно производить аудит и мониторинг системы. Чтобы свести к минимуму риск, связанный с халатностью пользователей (как показывает практика, это один из серьезных рисков для безопасности информации в любом предприятии), применять персональную аутентификацию. Любой сотрудник может подключиться к информационным ресурсам корпорации только после персональной аутентификации.

Не менее актуальна для корпорации задача защиты от внешних угроз, например вирусных атак. Быстрая установка программных заплат для Windows. Это нетривиальная задача. Исправленные фрагменты кода должны рассылаться по всей корпорации автоматически.