УДК 004.056

А. В. Ревнивых, **А. М. Федотов**

Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

E-mail: alexchr@mail.ru; fedotov@sbras.ru

ОБЗОР ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ *

Работа посвящена описанию и анализу политик информационной безопасности в корпоративной системе. Под информационной безопасностью понимается защищенность информационных ресурсов (информационных систем) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информационных ресурсов. Одним из важнейших аспектов информационной безопасности является политика предприятия по ее обеспечению.

Ключевые слова: информационная безопасность, политики, риски, классификация угроз, доступ к информации, распределенные информационные ресурсы.

Введение

Глобальная информатизация постиндустриального общества привела к тому, что корпоративные информационно-телекоммуникационные системы приобрели важнейшее значение в современном мире. Корпоративные информационно-телекоммуникационные системы предназначены для получения определенных информационных услуг. Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Поэтому важнейшим элементом информационной безопасности является доступность тех или иных сервисов информационных систем.

Понятие информационной безопасности, введенное по аналогии с государственной безопасностью или энергетической безопасностью, – это защищенность информационных ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информационных ресурсов и поддерживающей инфраструктуры [1]. В контексте данной работы *система информационной безопасности в корпоративной сети* понимается как совокупность организационных мер и технологических решений для обеспечения доступности, целостности (актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения) и конфиденциальности (в том числе и защита от несанкционированного доступа).

В свете приведенного определения основные задачи информационной безопасности можно сформулировать как:

* Работа выполнена при поддержке РФФИ (проекты № 12-07-00472, 11-07-00561, 10-07-00302), а также проекта ФЦП № 2012-1.4-07-514-0022-004.

- обеспечение надежного функционирования информационных систем и предоставляемых ими услуг, создание технологической и материально-технической базы информационной безопасности;
- создание механизмов своевременного выявления, прогнозирования, локализации и оперативного реагирования на угрозы безопасности и проявления негативных тенденций в использовании информационных ресурсов и систем;
- анализ и оценка рисков нарушения информационной безопасности;
- создание эффективных регламентирующих документов эксплуатации информационных ресурсов и нормативных документов обеспечения информационной безопасности;
- обеспечение правовой защиты субъектов информационных отношений;
- сохранение и эффективное использование информационных ресурсов;
- координация деятельности субъектов информационного обмена в обеспечении информационной безопасности;
- унификация требований к обеспечению информационной безопасности [2].

Отметим, что проблемы информационной безопасности затрагивают все уровни научно-технологического обеспечения – от теоретических основ и международных стандартов до оперативного администрирования. Как видим, из приведенного списка задач на важнейшее место выходит задача определения и разработка политик (регламентов и нормативных документов), связанных с информационной безопасностью (ИБ), а также дальнейшее соблюдение этих регламентов. Необходимость формализованной политики информационной безопасности в настоящее время является одним из определяющих факторов функционирования информационных систем.

Главной причиной появления политики безопасности обычно является требование наличия такого документа от регулятора – организации, определяющей правила работы предприятий данной отрасли. В этом случае отсутствие политики может повлечь репрессивные действия в отношении предприятия или даже полное прекращение его деятельности.

Кроме того, определенные требования (рекомендации) предъявляют отраслевые или общие, местные или международные стандарты. Обычно это выражается в виде замечаний внешних аудиторов, проводящих проверки деятельности предприятия. Отсутствие политики вызывает негативную оценку, которая в свою очередь влияет на публичные показатели предприятия — позиции в рейтинге, уровень надежности и т. д.

Еще одной причиной является внутреннее осознание руководством предприятия необходимости структурированного подхода к обеспечению определенного уровня безопасности. Обычно такое осознание наступает после внедрений ряда технических решений по безопасности, когда возникают проблемы управления такими решениями. Иногда сюда добавляются вопросы обеспечения безопасности персонала (Human Resources Security, куда входит как защита самих работников, так и защита от них), юридические аспекты и другие факторы, приводящие руководство предприятия к пониманию того, что обеспечение информационной безопасности выходит за рамки чисто технических мероприятий, проводимых ИТ-подразделением или другими специалистами.

Интересно, что, согласно исследованию по безопасности, проведенному компанией Deloitte в 2006 г., предприятия, которые имеют формализованные политики информационной безопасности, значительно реже подвергаются взлому. Это свидетельствует о том, что наличие политики является признаком зрелости предприятия в вопросах информационной безопасности. То, что предприятие внятно сформулировало свои принципы и подходы к обеспечению информационной безопасности, означает, что в этом направлении была проделана серьезная работа.

Стандарты и рекомендации, рассмотренные в [3; 4] [1], образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности. В то же время этот базис ориентирован, в первую очередь, на производителей и «оценщиков» систем и в гораздо меньшей степени на потребителей [1].

[1] ГОСТ Р ИСО / МЭК 15408-1(2,3)-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

При анализе рисков нарушения ИБ становится очевидным, что на ИБ организации в конечном счете влияет соблюдение очень широкого спектра различного рода политик, регламентирующих действия сотрудников и контрагентов организации с точки зрения совершенно разных аспектов. Кроме того, в политике ИБ может регламентироваться поведение в различных ситуациях самой информационной системы (ИС) и ее отдельных компонентов в частности [5].

Риски нарушения ИБ для разных организаций будут отличаться как номенклатурно, так и качественно. Необходимо также отметить, что один и тот же инцидент может по-разному трактоваться каждым из субъектов, если к нему имеют то или иное отношение несколько организаций. Относительность толкований проявляется и на больших предприятиях, где существенный ущерб одного из структурных подразделений может и не особо повлиять на деятельность головного предприятия (и, наоборот, для структурного подразделения ущерб может казаться небольшим, но для всего предприятия окажется трагедией).

Важным аспектом при разработке политик ИБ является баланс между затратами на ИБ и возможным ущербом, а также его вероятностью.

Сложность ИС и затраты на ИБ. Затраты на ИБ могут быть материальными и нематериальными (временны́ми, интеллектуальными) и начинаются еще на ранних стадиях разработки ИС, когда используются сочетания уже готовых технологий ИБ, а также новые решения. Реализациями технологий являются совокупности оборудования, программного обеспечения (ПО) и определенных политик использования комплексов для обслуживающего персонала и пользователей ИС. Стоимость современных средств защиты зависит от их качества и необходимого количества, которые в свою очередь определяются в зависимости от величины, сложности и критичности защищаемой ИС.

Величина и сложность защищаемой ИС обычно являются связанными понятиями. Например, простое увеличение числа однотипных рабочих станций в сети с неизменной топологией уже можно считать усложнением системы, так как конфигурация двух компьютеров недолго может оставаться абсолютно идентичной. Кроме того, в больших сетях часто встречаются отклонения от нормального режима работы программно-аппаратной среды передачи данных, которые можно объяснить лишь банальной величиной и сложностью локальной сети.

Чем больше размер и сложность ИС, тем более дорогие средства защиты приходится использовать [1].

Любые регламентирующие документы (в том числе политики ИБ организации) вводят определенные ограничения на возможности информационной системы и взаимодействие с ней пользователей и других информационных систем. Чем больше ограничений вводится, тем, очевидно, в большей степени страдает удобство пользования и, в конечном счете, производительность системы, а также ее пользователей. Проиллюстрировать это можно увлечением авторов системы безопасности беспрестанно идентифицировать пользователей [2], когда перед каждым малозначительным действием нужно ввести имя и пароль для очередного подтверждения полномочий. Таким образом, работа пользователя превращается в основном во введение идентификационных данных, а не в производительный труд с сущностью ИС. Если предположить, что пароли для каждого конкретного действия еще и отличаются, то производительная работа пользователя может быть попросту блокирована. В подобных случаях пользователи нередко начинают саботировать применение средств ИБ.

Ограничение функциональности системы по обмену информацией с другими ИС приводит в целом к уменьшению ее потенциальных возможностей. Понятие о критичности ИС связано с критичностью последствий от временного или постоянного нарушения ее ИБ.

Ущерб от нарушения ИБ. Классифицировать ущерб будем с точки зрения двух критериев: критичности и вероятности.

Критичность ущерба от нарушения ИБ для каждой конкретной ИС различна. Более того, даже для одной и той же системы критичность может различаться в зависимости от момента времени нарушения ИБ. Например, для структурного подразделения организации, выпол-

[2] Если не реализована концепция единой точки доступа в сеть и работа с сертификатами, например, на основе протокола LDAP.

няющего функции бухгалтерии, наиболее неблагоприятный момент для нарушения работоспособности системы – отчетные периоды; исправная ИС самолета наиболее необходима пилотам во время взлета и посадки воздушного судна.

Предлагается классифицировать организации по критерию глубины проникновения ИС в их основную деятельность на три категории.

1. Организации, основной продукт деятельности которых напрямую не зависит от ИС.
2. Организации, основной продукт деятельности которых напрямую от ИС не зависит, но управление его созданием происходит за счет ИС.
3. Организации, продуктом деятельности которых являются новые ИС.

При этом необходимо отметить, что ИС активно используются в любых официально зарегистрированных современных организациях (это достигнуто на законодательном уровне). Поэтому представителям даже первой категории необходимо учитывать, что, например, для учета и отчетности организации наверняка используют АРМы на базе «1С Предприятия» или других аналогичных продуктов. Тем не менее чем ближе ИС к основному предмету деятельности организации, тем, очевидно, больший относительный ущерб доставит нарушение режима ИБ при прочих равных условиях.

Нарушения могут быть связаны с любым из аспектов ИБ: доступностью, конфиденциальностью или актуальностью / целостностью. Однако для разных организаций критичность нарушения каждого из аспектов разная. Например, для ресурса, который размещает в открытом доступе прогноз погоды на коммерческой основе, нарушение критерия конфиденциальности вряд ли будет критичным, в то время как нарушение доступности или актуальности / целостности очень критично.

Вероятность ущерба от инцидентов, связанных с нарушением режима ИБ, очевидно, зависит от вероятности возникновения соответствующих инцидентов, но при этом надо учитывать, что в зависимости, например, от момента нарушения ИБ сколько-нибудь существенный ущерб от инцидента может и не возникнуть даже при серьезных нарушениях.

Необходимо отметить, что в современных условиях для большинства организаций нарушение доступности ресурсов приводит к большему ущербу, чем нарушения, связанные с утратой конфиденциальности. Немаловажно, что нарушения доступности относительно критично для всех организаций, в отличие от конфиденциальности или актуальности. Кроме того, при отказе от обслуживания всегда возникает моральный ущерб.

Политики информационной безопасности

Вероятностью возникновения инцидентов нарушения ИБ и ущербом от них можно управлять. Для этого предназначены политики ИБ. В данной работе термин «политика информационной безопасности» означает совокупность правил, организационно-технических и режимных мер и методов, определяющих и ограничивающих виды деятельности объектов и субъектов, системы информационной безопасности. Вероятность инцидентов нарушения ИБ и их критичность, по сути, зависят от степени проработанности принятых в организации политик ИБ и степени их соблюдения всеми сотрудниками.

Как было отмечено, политики ИБ весьма связаны и потому должны быть интегрированы с другими политиками организации. Например, кадровая политика определяет как уровень начальных требований к потенциальным пользователя ИС предприятия, так и необходимость соблюдать политику ИБ, способы контроля за соблюдением политики ИБ, а также меры ответственности за инциденты, приводящие (или могущие привести) к нарушениям ИБ.

Важную роль для политики ИБ играет интеграция с политикой физической безопасности. Для обеспечения неприкосновенности данных, хранящихся и обрабатываемых в ИС, а также для выполнения требования доступности необходимо ограничивать физический доступ к аппаратной части ИС. Абсолютное большинство всех способов обойти стандартные дистанционные средства авторизации программно-аппаратных компонентов современных ИС основаны на наличии физического доступа к ним. Кроме того, к физической безопасности можно отнести и защиту аппаратных компонентов ИС от нежелательных воздействий природных явлений и деятельности человека, даже напрямую не связанной с желанием нарушить режим ИБ организации.

Основной угрозой ИБ, с точки зрения ПО, является возможность обойти программным путем штатные средства авторизации ИС, а также недостатки механизмов проверки полномочий пользователей.

По основным механизмам функционирования политики ИБ можно разделить на две категории:

- политики технологического обеспечения;
- организационные политики.

Политики технологического обеспечения включают учет, эксплуатацию и защиту оборудования, ПО и информационных ресурсов. В свою очередь, они делятся на инфраструктурные (связанные с оборудованием, системным ПО и сетевыми сервисами) и прикладные (связанные с прикладным ПО и пользовательскими информационными ресурсами).

К политикам инфраструктурного технологического обеспечения относятся:

- политика учета инфраструктурных ресурсов;
- политика мониторинга инфраструктуры;
- политика предоставления и разграничения доступа к инфраструктурным ресурсам;
- политика обновления инфраструктуры;
- политика защиты от вторжений;
- политика обеспечения целостности информации;
- политика защиты от нарушений доступности;
- политика резервного копирования.

К политикам прикладного технологического обеспечения относятся:

- политика учета пользовательских ресурсов;
- политика мониторинга пользовательских ресурсов;
- политика предоставления и разграничения доступа к прикладным ресурсам;
- политика предоставления и разграничения доступа к информационным ресурсам;
- политика использования средств криптографической защиты;
- политика мониторинга прикладных ресурсов;
- политика обеспечения актуальности информации;
- политика обновления прикладных ресурсов.

Организационные политики регламентируют действия персонала организации. К ним относятся:

- кадровая политика;
- политика обеспечения конфиденциальности служебной информации;
- экономическая политика.

Аспекты, которые необходимо учитывать при формировании политик инфраструктурного и прикладного обеспечения, а также организационных политик, описаны далее.

Аспекты политики инфраструктурного технологического обеспечения

Политика учета инфраструктурных ресурсов. Для эффективного управления ресурсами необходимо четко представлять объект управления. Целесообразно иметь исчерпывающую схему соответствующей информационной системы, в которой бы четко фиксировалось количество и характеристики каждого вида ресурсов, способы взаимодействия модулей информационной системы друг с другом и с окружающими объектами и системами.

Информационные системы состоят из инфраструктурных ресурсов, которые можно классифицировать на несколько видов.

1. Вычислительные ресурсы характеризуются максимальным количеством операций, выполняемых информационной системой за определенный промежуток времени. Вычислительная мощность зависит от множества факторов:

- производительности (тактовой частоты, разрядности, количества физических и логических ядер, архитектуры, объема и быстродействия кэша) центрального процессора (таких процессоров в одной вычислительной системе может быть несколько);
- объема и быстродействия оперативной памяти;
- быстродействия используемых для загрузки / выгрузки данных дисковых накопителей, каналов связи, периферийных устройств (видеоадаптеров, звуковых карт и т. д.);

- быстродействия шин передачи данных, которыми соединены вышеупомянутые устройства между собой;
- системного ПО, прикладного ПО, а также драйверов устройств (важны как технические возможности программных компонентов, так и их настройки).

Необходимо отметить, что в целом величина вычислительных ресурсов зависит не только от количественных и качественных показателей быстродействия этих программно-аппаратных компонентов ИС, но и от их совместимости между собой. Например, никакого существенного прироста производительности не предвидится при использовании полностью 64-разрядной аппаратной платформы в сочетании с 32-разрядным программным обеспечением, так как вычислительные возможности оборудования просто не смогут быть полностью задействованы на уровне ПО. Аналогичный пример касается и многоядерных или многопроцессорных систем, в которых при использовании не предназначенного для работы в многоядерной среде ПО возможен эффект снижения производительности за счет того, что все задачи будут возложены на одно из физических ядер, а другие в это время будут простаивать.

2. Ресурсы хранения информации характеризуются максимальным объемом данных, который способна содержать в себе ИС на условиях длительного хранения. Максимальный объем хранения данных зависит от объема стационарных и подключаемых накопителей информации, входящих в состав ИС. При этом максимальный объем данных для хранения в ИС не совпадает с суммарным объемом всех подключаемых к системе накопителей, так как неизбежно дублирование данных в одной и той же ИС, например, связанное с необходимостью их резервного копирования.

3. Ресурсы передачи данных характеризуются технической возможностью и скоростью взаимодействия системы с другими объектами. Ресурсы передачи данных включают аппаратную и программную части.

3.1. Аппаратные ресурсы характеризуются максимальной пропускной способностью и скоростью реакции (а также принципиальным наличием и стабильностью работы) каналов связи ИС с внешними объектами (например, с другими ИС) на уровне оборудования.

3.2. Программные ресурсы характеризуются наличием технической возможности и максимальной скоростью обмена информацией с другими объектами на уровне программного обеспечения. Программное обеспечение в данном случае может быть трех видов:

- программные протоколы передачи данных транспортного уровня;
- инфраструктурные сервисы;
- сервисы пользовательского уровня.

Единицей измерения ресурсов передачи данных является максимальное количество информации (измеряемое в битах), которым ИС может обмениваться по определенному каналу связи в течение секунды времени. Физических каналов связи у одной ИС может быть несколько. Кроме того, в рамках одного физического канала связи ИС может обмениваться информацией одновременно с использованием нескольких программных сетевых протоколов.

4. Ресурсы обеспечения отказоустойчивости и безопасности характеризуются вероятностью нарушения режима ИБ в ИС с точки зрения любого из критериев (доступности, актуальности, целостности и конфиденциальности). Вероятность нарушения режима ИБ в ИС зависит от наличия и эффективной конфигурации средств обеспечения отказоустойчивости (в том числе сетевых фильтров, источников бесперебойного питания, охлаждения, резервного копирования и т. д.), целостности и актуальности, а также конфиденциальности (в том числе бескомпромиссной аутентификации, антивирусного ПО, сетевых брандмауэров, шифрования и т. д.). Ресурсы тем больше, чем меньше вероятность нарушений. Важно отметить, что достоверно оценить вероятность нарушения режима ИБ практически невозможно, поэтому организациям приходится снижать до возможного минимума чисто гипотетическую вероятность нарушений, которую было бы эффективно измерять в процентах или долях единицы в случае, если бы ее можно было достоверно оценить.

5. Периферийные ресурсы характеризуются количеством и техническими данными периферийных устройств. К таким ресурсам отнесем устройства ввода (сканеры, факсовые аппараты, микрофоны и т. д.) и вывода (принтеры, плоттеры, акустические системы, проекторы и т. д.). Оценка периферийных ресурсов может быть количественной (наличие и количество

ресурсов определенного вида) и качественной (возможности, предоставляемые имеющимися ресурсами).

Составные части ИС подлежат простому количественному учету с точки зрения программных и аппаратных компонентов, из которых они состоят, хотя такой учет имеет к ИБ лишь косвенное отношение. Тем не менее в бухгалтерии организации должна иметься информация о количестве каждого из видов оборудования и ПО, а также о закреплении их за тем или иным структурным подразделением и конкретным сотрудником.

Основной целью реализации политики учета инфраструктурных ресурсов является грамотное распределение всех видов ресурсов между решаемыми задачами в соответствии с установленными приоритетами их выполнения, а также создание возможности для поддержания ресурсов в исправном и доступном состоянии.

Политика мониторинга инфраструктуры. Мониторинг инфраструктурных ресурсов ИС должен производиться для проверки их работоспособности в рамках назначения. Основной задачей, решаемой при настройке системы мониторинга, должна быть как можно большая автоматизация.

Мониторинг аппаратных ресурсов производится для выявления следующих аспектов.

- Доступность ресурсов оборудования. Подразумевает принципиальную возможность использования по назначению.
- Степень работоспособности. Работоспособность вычислительной техники может меняться в зависимости от внешних и внутренних факторов. Например, на скорость вычислений центральных процессоров влияет их температура, которая в свою очередь зависит от множества факторов, таких как температура окружающей среды, интенсивность нагрузки на систему, исправность и эффективность системы охлаждения и т. д.
- Степень износа. Риск выхода из строя велик на ранних стадиях эксплуатации нового оборудования и наоборот, когда оборудование эксплуатируется долго (больше гарантийного срока). Износ определяется сроком эксплуатации, а также ее условиями и интенсивностью.
- Эффективность использования. Разные типы оборудования имеют различные эффективные диапазоны нагрузок. Например, бытовые источники бесперебойного питания не рекомендуется нагружать по мощности подключаемого к ним оборудования более чем на половину их вольт-амперной характеристики. При этом в процессе мониторинга должны выявляться и простаивающие компоненты оборудования.

Мониторинг программных ресурсов производится для выяснения следующих аспектов.

- Доступность и целостность инфраструктурных программных сервисов. Проверяется, загружена ли операционная система, правильно ли отвечают на запросы сервисы, все ли сервисы доступны.
- Степень работоспособности. Определяется скоростью и корректностью работы программных инфраструктурных сервисов, которая зависит от множества факторов, среди которых: исправность оборудования, интенсивность использования оборудования, интенсивность использования ПО, корректность программной конфигурации ИС (наличие и корректность всех необходимых библиотек, отсутствие в системе активных вредоносных программ, объем и непротиворечивость реестра настроек ИС).
- Эффективность использования. Инфраструктурное ПО имеет определенный эффективный диапазон нагрузок, который не следует превышать. Например, превышение определенного количества одновременных запросов к серверу баз данных будет вызывать нарушения доступности соответствующего сервиса. При этом немаловажно, что после определенного количества запросов в единицу времени наступление условий ограничения производительности сервера баз данных уже не будет зависеть от степени загруженности аппаратных ресурсов. При этом в процессе мониторинга должны выявляться и простаивающие компоненты ПО.
- Актуальность. Программное обеспечение нуждается в регулярном обновлении как для соответствия запросам современного прикладного ПО, так и для освобождения от найденных уязвимостей.

Политика предоставления и разграничения доступа к инфраструктурным ресурсам. Инфраструктурные ресурсы классифицируем на два типа: общесистемные и пользовательские. К общесистемным ресурсам отнесем серверы (аппаратные и программные), сетевые сервисы,

ядро сети передачи данных (кабели, свитчи, маршрутизаторы, каналы доступа к внешним сетям) т. д. К пользовательским инфраструктурным ресурсам – оборудование и системное ПО, установленные на рабочих местах пользователей.

Общесистемные аппаратные ресурсы имеет смысл эксплуатировать в специально оборудованных помещениях для исключения физического доступа к ним неквалифицированного персонала, а также злоумышленников. В политике ИБ имеет смысл предусмотреть определенный режим доступа к серверным помещениям, в котором учитывается круг лиц, которым разрешен вход в такие помещения, а также регистрация входа и выхода из помещения.

Очевидно, что пользовательские аппаратные ресурсы должны быть доступны, как минимум, их пользователям. Но даже в этом случае существуют способы контролировать этот доступ (программно-аппаратные комплексы мониторинга, видеонаблюдение, опломбирование и т. д.).

У всех пользователей, кроме системных администраторов, должен отсутствовать доступ к системному ПО, установленному на серверах и других общесистемных ресурсах. Кроме того, у системных администраторов, если их в организации несколько, должен быть доступ только к тем ресурсам, доступ к которым нужен для выполнения служебных обязанностей.

Доступ к системному ПО, установленному на рабочих станциях пользователей, должен регламентироваться исходя из квалификации пользователя и его служебных обязанностей. В любом случае пользователи не должны сами заниматься переустановкой операционных систем, иметь доступ к тем возможностям системы, к которым доступ необязателен для выполнения служебных обязанностей.

Политика обновления инфраструктуры. Оборудование и системное ПО должны регулярно обновляться. Необходимость замены оборудования связана с его моральным устареванием, износом, а также непрекращающейся тенденцией увеличения запросов программного обеспечения к ресурсам оборудования.

По отношению к оборудованию основных целей обновления две: моральное устаревание и физический износ.

Возможно три основных стратегии обновления оборудования: аварийная, плановая, аварийно-плановая.

- При аварийной стратегии обновления оборудования оно заменяется новым только в случае серьезной поломки, при которой чинить аппаратные компоненты становится нецелесообразным в силу экономических или каких-либо других причин. Профилактическая замена оборудования на новое не предусматривается. Кроме того, возможна внеплановая замена оборудования, если оно категорически перестает устраивать по производительности или каким-то другим характеристикам.
- При плановой стратегии обновления оборудования каждому аппаратному компоненту устанавливается срок службы, по истечению которого этот компонент обязательно заменяется новым. При поломке ранее этого срока возможность замены на полностью новое оборудование не предусматривается, заменяются лишь неисправные элементы, либо же неисправный комплект полностью выводится из эксплуатации до наступления срока планового обновления.
- В большинстве случаев используется аварийно-плановая стратегия обновления, которая предусматривает сочетание установки максимальных сроков службы аппаратных компонентов, но при этом не исключает их замены на новые в случае значительных неисправностей или неожиданного категорического морального устаревания до истечения планового срока эксплуатации.

По отношению к системному ПО выделим две основных стратегии обновления: по уязвимости и моральному устареванию.

- Обновление по уязвимости производится для устранения ошибок и недоработок системного ПО, которые могут приводить к сбоям в работе ПО, а также потенциальным уязвимостям системы. Обычно производители системного ПО выпускают регулярные обновления, установка которых может производиться вручную или автоматически.
- Моральное устаревание системного ПО происходит обычно при выходе новой версии используемой программно-аппаратной платформы. При этом далеко не всегда целесообразно обновлять операционную систему до следующей версии непосредственно после ее появле-

ния. Производители обычно продолжают техническую поддержку и выпуск обновлений для предыдущих версий системного ПО в течение нескольких лет после появления новых версий.

Характерным следствием любых обновлений оборудования и системного ПО является временная неработоспособность обновляемой части системы или всей системы. Для обновления аппаратных компонентов оборудование необходимо выключать, после обслуживания компонентов системного ПО обычно требуется перезагрузка операционной системы.

Необходимо отметить также и тот факт, что при каждом обновлении как оборудования, так и системного ПО существенно повышается риск отказа в работе обновленной системы – нет исчерпывающей гарантии, что обновление будет установлено штатно и, кроме того, новый компонент оборудования или системного ПО всегда обладает меньшим временем тестирования, поэтому возникновение непредвиденных проблем с ним вполне возможно.

Политика защиты от вторжений. Под вторжением в ИС будем понимать несанкционированный доступ к ее компонентам.

Защиту от вторжений можно разделить на три уровня: аппаратный, программно-локальный, программно-удаленный. Все эти уровни тесно взаимосвязаны, поэтому в случаях реальных вторжений часто используются совместно.

- Аппаратный уровень защиты от вторжений подразумевает защиту физических компонентов ИС от несанкционированного взаимодействия. Многие виды телекоммуникационного оборудования обладают надежной защитой от вторжений на программном уровне, но при этом рассчитаны на то, что физический доступ к ним неавторизованные лица не получат ни при каких обстоятельствах. Типичным примером важности защиты аппаратных компонентов может являться надежность пароля на включение персонального компьютера, ввод которого проблематично обойти при условии невозможности вскрытия системного блока с целью, например, удалить из материнской платы батарейку, обеспечивающую питание той части памяти, в которой хранится пароль. Кроме того, для некоторых программных вторжений даже внешний вид серверной стойки может оказаться полезным с точки зрения познания структуры компьютерной сети организации, типов и версий используемого активного сетевого оборудования. Отметим, что само по себе вторжение на аппаратном уровне вряд ли интересует злоумышленников и является лишь промежуточным подготовительным этапом для вторжений на программном уровне.
- Программно-локальный уровень защиты подразумевает обеспечение безопасности на рабочих станциях и серверах ИС от вторжений с использованием потенциальных локальных уязвимостей системного и прикладного ПО. Современное программное обеспечение содержит значительное количество разнообразных уязвимостей, например, связанных с потенциальной возможностью срыва стека. В связи с этим необходимо обеспечивать регулярное обновление программного обеспечения рабочих станций ИС актуальными версиями, кроме того, не допускать появления у пользователей полномочий, которые им необязательно иметь для исполнения своих служебных обязанностей. Серверы целесообразно размещать в отдельном помещении с ограниченным доступом для исключения возможности локального взаимодействия злоумышленников с серверным оборудованием и ПО.
- Программно-удаленный уровень защиты подразумевает обеспечение безопасности на рабочих станциях и серверах ИС от удаленных вторжений. Удаленными вторжениями можно считать несанкционированные попытки взаимодействия с ПО серверов и рабочих станций из периметра локальной сети организации, а также не из пределов периметра (например, из сети Internet). Защита от вторжений из периметра локальной сети сводится в основном к профилактическим мероприятиям (исключение возможности появления у пользователей необязательных для исполнения их служебных обязанностей полномочий в системе, установка межсетевых экранов, фильтров, обновление сетевого программного обеспечения серверов и рабочих станций, системы мониторинга и т. д.). Защита от вторжений не из контролируемого периметра включает запрет на удаленный доступ к рабочим станциям, регулярное обновление сетевого программного обеспечения серверов, установку межсетевых экранов, фильтров, системы мониторинга трафика, отключение необязательных сетевых сервисов на серверах.

Политика обеспечения целостности информации. Под целостностью информации в данном случае будем понимать совокупность двух аспектов: неизменности и полноты.

- Неизменность информации подразумевает отсутствие возможности изменения информации несанкционированными или ошибочными действиями пользователей. Обратим внимание на тот факт, что опасность от использования некорректных данных может быть даже выше, чем полная потеря данных и, следовательно, невозможность их использования для принятия решений.
- Полнота информации является важным аспектом целостности. Например, если одной из функций ИС является выдача пользователям прогноза погоды, то от его полноты будет зависеть ценность выдаваемой информации. Например, если будет выдан прогноз погоды, но не будет указано, на какое число этот прогноз, то это сделает невозможным практическое применение такого прогноза. Для обеспечения полноты информации необходимо четко налаживать схемы взаимодействия между компонентами ИС, которые отвечают за формирование каждой части от полного комплекта данных.

Политика защиты от нарушений доступности. Ущерб от нарушений доступности информации в большинстве случаев даже выше, чем от нарушений конфиденциальности, например. Для обеспечения доступности необходимо предусматривать широкий спектр мер, включая резервирование электроснабжения ИС, каналов связи между компонентами ИС и внешним миром, использование в ИС как можно более надежных и проверенных компонентов, дублирование особо важных или заведомо ненадежных компонентов, назначение и тщательное исполнение регламентов профилактических работ с оборудованием и программным обеспечением, из которых состоят компоненты ИС, разработка планов действий в нештатных ситуациях для персонала и т. д.

Политика резервного копирования. Резервное копирование информации является насущной необходимостью, так как никакие меры по обеспечению доступности и целостности не могут гарантировать на 100 % ее защиту от уничтожения или несанкционированного изменения.

Резервное копирование может осуществляться автоматическим методом по расписанию или фиксации определенных событий в системе, а также вручную.

При разработке графика резервного копирования приходится сталкиваться с необходимостью соблюдать баланс между затратами на резервное копирование и потенциальными затратами на восстановление информации в случае, если исходный носитель пострадает. Очевидно, что чем чаще производится резервное копирование, тем меньше вероятность безвозвратно потерять важные данные с момента последнего резервирования и, следовательно, меньше затраты на восстановление ИС в работоспособное состояние с актуальными и цельными данными.

Однако каждый раз для резервного копирования необходимо выделять определенное (обычно довольно значительное) время, место на носителях. Во многих случаях во время резервного копирования данных работа с системой затруднена или вообще противопоказана, поэтому в целом отметим, что слишком частые операции по резервному копированию отрицательно влияют на общую производительность труда пользователей ИС.

Для резервного копирования предусматривается определенное расписание, носители, правила ротации носителей, количество копий, глубина истории копий (сколько последовательных последних копий данных сохраняется).

Аспекты политики прикладного технологического обеспечения

Политика учета пользовательских ресурсов. Прикладные ресурсы характеризуются наличием и эффективностью алгоритмов, реализованных в виде прикладного ПО, для решения определенных задач и зависят от назначения и возможностей имеющегося в ИС специализированного прикладного ПО, а также от поддержки функций ПО оборудованием.

Интерфейс прикладного ПО может предусматривать возможность взаимодействия как с пользователем, так и с другими прикладными программами.

Прикладные ресурсы тем больше, чем выше эффективность решения задач, поставленных перед ИС. Эффективность может оцениваться с точки зрения различных критериев:

- круг решаемых ИС задач;
- скорость решения задач;
- точность расчетов при решении задач;
- достоверность результатов (зависит не только от точности расчетов, но и от правильного выбора исходных данных для расчетов, а также интерпретации полученных результатов);
- «глубина» решения задач (целостность и актуальность решения).

Алгоритмические ресурсы подлежат количественной оценке лишь при выборе конкретного критерия эффективности, поэтому у них не имеется общепринятой единицы измерения.

1. Информационные ресурсы характеризуются количеством и качеством информации, которая доступна в ИС. Технически доступ к информационным ресурсам производится через систему общего доступа к носителям, web-порталы или специализированное прикладное ПО.

Единицей измерения информационных ресурсов является объем в байтах, а также количество в штуках. Качественную оценку информационных ресурсов можно провести с точки зрения достоверности и актуальности.

Политика мониторинга пользовательских ресурсов. Мониторинг программных ресурсов производится для выяснения следующих аспектов.

- Доступность и целостность пользовательских программных сервисов. Проверяется, загружена ли прикладная программа, правильно ли отвечает на запросы.
- Степень работоспособности. Определяется скоростью и корректностью работы программных инфраструктурных сервисов и оборудования, исправностью оборудования, интенсивностью использования оборудования, интенсивностью использования ПО, корректностью программной конфигурации ИС (наличие и корректность всех необходимых библиотек, отсутствие в системе активных вредоносных программ, объем и непротиворечивость реестра настроек инфраструктурного ПО и прикладного).
- Эффективность использования. Прикладное ПО имеет определенный эффективный диапазон нагрузок, который не следует превышать. После определенного количества запросов в единицу времени наступление условий ограничения производительности прикладной программы уже не будет зависеть от степени загруженности аппаратных ресурсов. При этом в процессе мониторинга должны выявляться и простаивающие компоненты ПО.
- Актуальность. Программное обеспечение нуждается в регулярном обновлении как для соответствия запросам современного прикладного ПО, так и для освобождения от найденных уязвимостей. Кроме того, производители прикладного ПО в новых версиях своих продуктов, как правило, добавляют новые возможности, которые тоже имеет смысл отслеживать.

Политика предоставления и разграничения доступа к прикладным ресурсам. Прикладные ресурсы классифицируем на два типа: общесистемные и пользовательские. К общесистемным ресурсам отнесем прикладное ПО, установленное на серверах. К пользовательским прикладным ресурсам – прикладное ПО, установленное на рабочих местах пользователей.

Доступ к прикладному ПО, установленному на рабочих станциях пользователей и серверах, должен регламентироваться исходя из квалификации пользователя и его служебных обязанностей. В любом случае пользователи не должны сами заниматься переустановкой прикладных программ, иметь доступ к тем возможностям системы, к которым доступ необязателен для выполнения служебных обязанностей.

В отношении уровня доступа к возможностям прикладного ПО, установленного как на серверах, так и на рабочих местах пользователей, определенные ограничения эффективно накладывать и на системных администраторов, так как в большинстве случаев для выполнения своих служебных обязанностей полный доступ ко всем возможностям прикладного ПО им не нужен.

Политика использования средств криптографической защиты. Криптографическая защита подразумевает применение шифрования при хранении, обработке и передаче данных [6].

Криптография значительно затрудняет злоумышленникам перехват идентификационных данных (имени пользователя и пароля) пользователей ИС, а также любое использование данных, полученных с зашифрованных носителей или каналов передачи. В основном крипто-

графические методы используются для защиты от нарушений конфиденциальности информации. При этом обратим внимание на то, что в целом внедрение шифрования усложняет ИС, требует дополнительных вычислительных ресурсов для выполнения операций шифрования-дешифрования и, следовательно, отрицательно влияет на аспект доступности ИС и информации в ней.

Политика мониторинга прикладных ресурсов. Необходимость мониторинга прикладных ресурсов обуславливается их большим количеством и разнообразием. Мониторинг прикладных ресурсов должен производиться с точки зрения следующих аспектов: доступности, целостности, конфиденциальности, полномочий доступа.

Под прикладными ресурсами будем понимать ресурсы, к которым открыт общий доступ с определенными полномочиями (сетевые каталоги на серверах и рабочих станциях, сетевые принтеры, сканеры, ресурсы сети Интернет т. д.). Доступ к ресурсам осуществляется по определенным матрицам доступа, которые также являются объектом мониторинга.

Мониторинг должен осуществляться автоматически по определенному расписанию. В отличие от операции резервного копирования мониторинг не связан с существенными затратами вычислительных ресурсов ИС, снижением производительности труда пользователей, а потому может выполняться часто.

Мониторинг подразумевает также определенные действия в случае нарушения вышеперечисленных аспектов, с точки зрения которых мониторинг производится. Например, информирование о найденных проблемах системного администратора.

Политика обеспечения актуальности информации. Актуальность информации, обрабатываемой в ИС, должна постоянно поддерживаться за счет налаженной системы обновлений. В приведенном выше примере с прогнозом погоды, в подавляющем числе случаев, интересен только прогноз погоды на будущие периоды. Соответственно данные необходимо постоянно актуализировать.

Возможность актуализации в свою очередь зависит от доступности источников, из которых можно обновить и пополнить данные.

Политика обновления прикладных ресурсов. Прикладное ПО, наряду с системным, нуждается в обновлениях по нескольким причинам: моральное устаревание, обнаружение уязвимостей.

- Моральное устаревание прикладного ПО может быть вызвано наличием запросов на новые функции, а также на нюансы работы уже реализованных возможностей со стороны его пользователей. Оно происходит обычно при выходе новой версии программы. При этом далеко не всегда целесообразно обновлять прикладную программу до следующей версии непосредственно после ее появления. Производители обычно продолжают техническую поддержку и выпуск обновлений для предыдущих версий прикладного ПО в течение нескольких лет после появления новых версий.
- Многие программы, которые вполне можно классифицировать как прикладные, имеют доступ к ресурсам сети. В некоторых случаях к этим программам можно даже подключаться по сети. Соответственно на прикладное ПО распространяется необходимость защиты от удаленных и локальных уязвимостей. Обновление по уязвимости производится для устранения ошибок и недоработок прикладного ПО, которые могут приводить к сбоям в работе ПО, а также потенциальным уязвимостям системы (при взломе прикладной программы в некоторых случаях злоумышленник получает доступ к системе с полномочиями той учетной записи, из-под которой была запущена прикладная программа). Обычно производители прикладного ПО выпускают регулярные обновления, установка которых может производиться вручную или автоматически.

Аспекты организационной политики

Кадровая политика. Обратим внимание на то, что ни один этап жизни ИС не обходится без человека. Неизбежны риски нарушения надежности и безопасности при эксплуатации информационных систем, задуманных, созданных и эксплуатируемых людьми и для людей [1]. Исходя из этого значение кадровой политики сложно преувеличить.

Кадровая политика должна распространяться как на людей, которые создают, настраивают, поддерживают в работоспособном состоянии, администрируют ИС, так и на рядовых пользователей. Кроме того, большое значение имеют вещи, на первый взгляд кажущиеся мелочами. Например, при уборке помещений, в которых размещены компоненты ИС, сотрудникам необходимо проявлять осторожность с кабелями, компьютерами и т. д. Как следствие, степень надежности и безопасности работы ИС зависит буквально от каждого сотрудника организации. Скажем, медработник, который не имеет собственного доступа к ИС, тоже посвоему влияет на нее, допуская к работе других сотрудников, которые уже взаимодействуют с системой непосредственно.

Политика обеспечения конфиденциальности служебной информации. Под служебной информацией будем понимать данные о строении ИС, информации, содержащейся в ней, распределении полномочий по доступу к ИС, способах обеспечения безопасности и другие данные, позволяющие воспользоваться конфиденциальной информацией или нарушить доступность и целостность компонентов ИС.

В данной политике должно предусматриваться четкое определение о том, какая именно информация относится к «служебной» и какие конкретно накладываются ограничения на ее распространение и использование. Кроме того, немаловажное значение имеет разработанная и применяемая система наказаний за нарушение конфиденциальности служебной информации.

Экономическая политика. Описанные в других политиках мероприятия, будь то обновление, мониторинг, обеспечение конфиденциальности и доступности, даже просто электропитание ИС и возможности ее собственных компонентов, зависят от выбранной экономической политики организации, так как требуют материальных ресурсов (как и сотрудники, которые занимаются внедрением и исполнением указанных мероприятий).

Немаловажно предусматривать в экономической политике и наличие резервов средств для непредвиденных ситуаций, так как в целом техника обладает общеизвестным свойством некоторой непредсказуемости.

Стратегии ИТ организации

В настоящее время на рынке ИТ возникли предпосылки к тому, что небольшим предприятиям становится невыгодно содержать собственную полноценную информационную инфраструктуру – с экономической точки зрения эффективнее ее арендовать. Выделим три варианта стратегий ИТ организаций.

- Собственная ИТ-инфраструктура. Сервера аппаратные и программные, кабельная или беспроводная локальная сеть передачи данных, средства резервного копирования информации и рабочие станции сотрудников находятся на балансе организации и обслуживаются силами специальных штатных сотрудников.
- Облачные вычисления (ОВ). Вычислительные ресурсы (и место для размещения информации) реализованы как корпоративно, так и арендуются у специализированных организаций. В таком случае доступ к ресурсам технически возможен из любой точки мира, где есть подключение к сети Internet, практически с любого компьютера. Персоналу организации нет нужды беспокоиться о доступности, целостности и в некоторых случаях даже конфиденциальности информации, так как выполнение требований по обеспечению данных аспектов ИБ берет на себя специализированная фирма-арендодатель или отдельное подразделение в самой организации.
- Центры обработки данных (ЦОД) – это способ организации собственной инфраструктуры для крупных организаций, который призван снизить эксплуатационные расходы на инфраструктуру ИС. Концепция безопасного использования ресурсов ИС для организации радикально меняется по сравнению с вариантом классической собственной ИТ-инфраструктуры.

Заключение

В последнее время в рамках построения системы информационной безопасности много внимания уделяется концепции ITSM (IT Service Management, управление услугами ИТ) – подмножество библиотеки ITIL, описывающее процессный подход к предоставлению информационных технологий и обеспечению их использования [7].

Приведенный выше подход к составлению обзора политик информационной безопасности в целом приводит к результатам, которые во многих отношениях коррелируют с тем, на что предлагается обратить внимание при внедрении концепции ITSM. Разница состоит в том, что ITSM рекомендует сосредоточиться на клиенте и его потребностях, на услугах, предоставляемых пользователю информационными технологиями, а не на самих технологиях. Описанный подход, напротив, в основном сосредоточен на технологиях и, кроме того, имеет весьма четко заявленную направленность на обеспечение, прежде всего, ИБ. В каком-то смысле подходы можно считать и противоположными друг другу, так как в целом внедрение политики ИБ обычно снижает удобство использования ИС для рядовых пользователей.

Список литературы

1. *Галатенко В. А.* Основы информационной безопасности. М., 2004. 264 с.

2. *Федотов А. М.* Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций / ВИНИТИ. М., 2008. № 2. С. 88–101.

3. Галатенко В. А. Стандарты в области безопасности распределенных систем // Jet Info. 1999. № 5. С. 16–19.

4. *Галатенко В. А.* Стандарты информационной безопасности. М., 2006. 208 с.

5. *Мазов Н. А., Ревнивых А. В., Федотов А. М.* Классификация рисков информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2011. Т. 9, вып. 2. С. 80–89.

6. *Бернет С., Пэйн С.* Криптография. Официальное руководство RSA Security. М.: Бином-Пресс, 2002. 384 с.

7. *Ингланд Р.* Введение в реальный ITSM: Пер. с англ. М.: Лайвбук, 2010. 132 с.

Материал поступил в редколлегию 18.07.2012

A. V. Revnivykh, A. M. Fedotov

REVIEW OF INFORMATION SECURITY POLICIES

This paper describes a review and analysis of information security policies in the corporate system. Under the information security means security of information resources (information systems) and supporting infrastructure from accidental or intentional exposure to natural or artificial, with the potential damage to the owners or users of information resources. One of the most important aspects of information security policy of the company is to secure it.

Keywords: information security policy, risk, classification of threats, access to information, distributed information resources.