Известия Гомельского государственного университета
имени Ф. Скорины, №4(19), 2003

УДК 681.3

Политики информационной безопасности предприятий

А.Б. Демуськов, В.А. Короткевич, Л.И. Короткевич

В данной статье речь пойдёт о политиках компьютерной безопасности предприятий, имеющих выход в Internet. Само понятие *информационная безопасность* имеет различное содержание для различных людей. Это может быть директива одного из руководителей организации по организации программы компьютерной безопасности, устанавливающая ее цели и назначающая ответственных за ее выполнение. Или это может быть решение начальника отдела в отношении безопасности электронной почты. Или это могут быть правила обеспечения безопасности для конкретной системы (подсистемы). Под политикой безопасности мы будем понимать совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. С практической точки зрения политику безопасности целесообразно подразделить на три уровня. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Режимная организация в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности. На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности. Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров. Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы. В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Примеры таких вопросов – отношение к передовым но, возможно, недостаточно проверенным технологиям, доступ к Internet, использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д. В "политический" документ необходимо включить информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь. Например, если для использования работником неофициального программного обеспечения нужно официальное разрешение, должно быть известно, у кого и как его следует получать. Если должны проверяться дискеты, принесенные с других компьютеров, необходимо описать процедуру проверки. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

При формулировке целей, политика нижнего уровня может ориентироваться из соо ражений целостности, доступности и конфиденциальности, но она не должна на них остана ливаться. Ее цели должны быть конкретнее. Например, если речь идет о системе расчета зар ботной платы, можно поставить цель, чтобы только работникам отдела кадров и бухгалтер позволялось вводить и модифицировать информацию. В более общем случае цели должн связывать между собой объекты сервиса и осмысленные действия с ними. Из целей выводят правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем д тальнее правила, чем более формально они изложены, тем проще поддержать их выполнен программно-техническими мерами. С другой стороны, слишком жесткие правила могут м шать работе пользователей, вероятно, их придется часто пересматривать. Руководству приде ся найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый ур вень безопасности, а работники не окажутся чрезмерно скованы. Обычно наиболее формальн задаются права доступа к объектам ввиду особой важности данного вопроса.

При принятии решений администраторы сталкиваются с проблемой выбора на осно учета принципов деятельности организации, соотношения важности целей и наличия ресу сов. Эти решения включают определение того, как будут защищаться технические и инфо мационные ресурсы, а также как должны вести себя служащие в тех или иных ситуация Необходимым элементом политики является принятие решения в отношении данного вопр са. Оно задаст направление деятельности организации. Для того чтобы политика была у пешной, важно, чтобы было обоснованно выбрано одно направление из нескольких возмож ных. Для того чтобы описать политику по данной области, администраторы сначала должн определить саму область с помощью ограничений и условий в понятных всем терминах. За тем, необходимо явно указать цель или причины разработки политики – это может помоч добиться её соблюдения. В отношении политики безопасности в Internet организации може понадобиться уточнение: охватывает ли эта политика все соединения, через которые ведетс работа с Internet. Эта политика также может определять: учитываются ли другие аспекты ра боты в Internet, не имеющие отношения к безопасности, такие как персональное использова ние соединений с Internet.

Как только предмет политики описан, даны определения основных понятий и рас смотрены условия применения политики, надо в явной форме описать позицию организаци (то есть решение ее руководства) по данному вопросу. Это может быть утверждение о раз решении или запрете пользоваться Internet и при каких условиях. И самое главное – при по ложительном решении вопроса о использовании Internet, документ должен уточнять, где как, когда и к чему применяется данная политика. Для такого сложного вопроса, как безо пасность в Internet, организации может потребоваться ввести ответственных за анали безопасности различных архитектур. Для некоторых видов политик может оказаться уместным описание, с некоторой степенью детальности, нарушений, которые неприемлемы и последствий такого поведения. Могут быть явно описаны наказания, и это должно быт увязано с общими обязанностями сотрудников в организации. Если к сотрудникам применяются наказания, они должны координироваться с соответствующими должностными лицами и отделами. Также может оказаться полезным поставить задачу конкретному отделу в организации следить за соблюдением политики. Для любой проблемной политики нужны ответственные консультанты, с кем можно связаться и получить более подробную информацию. А так как должности имеют тенденцию изменяться реже, чем люди, и занимающие, разумно назначить лицо, занимающее конкретную должность как консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим – системный администратор или сотрудник службы безопасности Они должны уметь разъяснять правила работы в Internet или правила работы на конкретной системе. Internet – это только один из множества способов, которыми организация обычно взаимодействует с внешними источниками информации. И политика Internet должна быть согласована с другими политиками в отношении взаимоотношений с внешним миром.

Internet – это как бы электронная дверь в организацию. В одну и ту же дверь может войти как добро, так и зло. Организация, территория которой открыта для входа, наверное, уже приняла решение на основе анализа рисков, что открытость либо необходима для выполнения организацией своих задач, либо угроза слишком мала, что ей можно пренебречь. Аналогичная логика применима к электронной двери. Тем не менее существуют серьезные отличия. Физические угрозы более привязаны к конкретному физическому месту. А связь с Internet – это связь со всем миром. Организация, чья территория находится в спокойном и безопасном месте, может разрешать вход на свою территорию, но иметь в отношении Internet строгую политику. Internet может быть формой для общения с обществом. Многие организации инструктируют сотрудников, как им вести себя с корреспондентами или среди людей при работе. Эти правила следовало бы перенести и на электронное взаимодействие. Internet это не единственная глобальная сеть. Организации используют телефонные сети и другие глобальные сети(например, SPRINT) для организации доступа удаленных пользователей к своим внутренним системам. При соединении с Internet и телефонной сетью существуют аналогичные угрозы и уязвимые места.

После разработки большого числа политик, директив или приказов необходимо посмотреть: соблюдают ли формально написанные документы. Если нет, то можно либо попытаться изменить сам процесс разработки документов в организации, либо оценить, где имеются проблемы с ее внедрением и устранять их. Во втором случае, вероятно, потребуется разработка дополнительных документов.

Как правило большинство политик определяют то, что хочет руководитель предприятия. А чтобы политика безопасности в Internet была эффективной, руководитель предприятия должен понимать, какой выбор нужно сделать и делать его самостоятельно. Обычно, если руководитель доверяет разработанной политике, она будет корректироваться с помощью неформальных механизмов.

Для эффективности политика должна быть наглядной. Наглядность помогает реализовать политику, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Презентации, видеофильмы, семинары, вечера вопросов и ответов и статьи во внутренних изданиях организации увеличивают ее наглядность. Программа обучения в области компьютерной безопасности и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно уведомить всех пользователей о новой политике. С ней также нужно знакомить всех новых сотрудников организации.

Политики компьютерной безопасности должны доводиться таким образом, чтобы гарантировалась поддержка со стороны руководителей подразделений, особенно если на сотрудников постоянно сыплется масса политик, директив, рекомендаций и приказов. Политика организации – это средство довести позицию руководства в отношении компьютерной безопасности и явно указать, что оно ожидает от сотрудников в отношении производительности их работы, действий в тех или иных ситуациях и регистрации своих действий.

Для того чтобы быть эффективной, политика должна быть согласована с другими существующими директивами, законами, приказами и общими задачами организации. Она также должна быть интегрирована и согласована с другими политиками организации. Одним из способов координации политик является согласование их с другими отделами в ходе разработки. Кроме того, все положения выработанных политик должны быть отражены в должностных инструкциях руководителей всех уровней.

Если целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности, то более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер, расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности;
- обеспечение безопасности в каждой функциональной области локальной сети;

- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Руководители подразделений должны отвечать за доведение положений политики безопасности до пользователей и за контакты с пользователями.

Администраторы локальной сети должны обеспечивать непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, что их защита построена в соответствии с общей политикой безопасности.

Пользователи обязаны использовать локальную сеть в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения со стороны персонала должны рассматриваться руководством для принятия мер вплоть до увольнения.

И в заключение примерные требования к должностным обязанностям должностных лиц.

Руководители подразделений обязаны:

- постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же делали их подчиненные;
- проводить анализ рисков, выявляя активы, требующие защиты, и уязвимые места систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты;
- организовать обучение персонала мерам безопасности. Обратить особое внимание на вопросы, связанные с антивирусным контролем;
- информировать администраторов локальной сети и администраторов сервисов об изменении статуса каждого из подчиненных (переход на другую работу, увольнение и т.п.);
- обеспечить, чтобы каждый компьютер в их подразделениях имел хозяина или системного администратора, отвечающего за его безопасность и имеющего достаточную квалификацию для выполнения этой роли.

Администраторы локальной сети обязаны:

- информировать руководство об эффективности существующей политики безопасности и о технических мерах, которые могут улучшить защиту;
- обеспечить защиту оборудования локальной сети, в том числе интерфейсов с другими сетями;
- оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попытках нарушения защиты. Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- использовать проверенные средства аудита и обнаружения подозрительных ситуаций;
- ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности;

- следить за новинками в области информационной безопасности, информировать о них пользователей и руководство;
- не злоупотреблять данными им большими полномочиями. Пользователи имеют право на тайну;
- разработать процедуры и подготовить инструкции для защиты локальной сети от зловредного программного обеспечения. Оказывать помощь в обнаружении и ликвидации зловредного кода;
- регулярно выполнять резервное копирование информации, хранящейся на файловых серверах;
- выполнять все изменения сетевой аппаратно-программной конфигурации;
- гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- периодически производить проверку надежности защиты локальной сети. Не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов обязаны:

- управлять правами доступа пользователей к обслуживаемым объектам;
- оперативно и эффективно реагировать на события, таящие угрозу;
- информировать администраторов локальной сети о попытках нарушения защиты;
- оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- регулярно выполнять резервное копирование информации, обрабатываемой сервисом;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- ежедневно анализировать регистрационную информацию, относящуюся к сервису;
- регулярно контролировать сервис на предмет зловредного программного обеспечения;
- периодически производить проверку надежности защиты сервиса. Не допускать получения привилегий неавторизованными пользователями.

Пользователи обязаны:

- знать и соблюдать законы, правила, принятые в организации, политику безопасности, процедуры безопасности;
- использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- использовать механизм защиты файлов и должным образом задавать права доступа;
- выбирать хорошие пароли, регулярно менять их. Не записывать пароли на бумаге, не сообщать их другим лицам;
- помогать другим пользователям соблюдать меры безопасности. Указывать им на замеченные упущения с их стороны;
- информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях;
- не использовать слабости в защите сервисов и локальной сети в целом;
- не совершать неавторизованной работы с данными, не создавать помех другим пользователям;
- всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей;
- обеспечивать резервное копирование информации с жесткого диска своего компьютера;

- знать принципы работы зловредного программного обеспечения, пути его проникновения и распространения, слабости, которые при этом могут использоваться;
- знать и соблюдать процедуры для предупреждения проникновения зловредного кода, для его обнаружения и уничтожения;
- знать слабости, которые используются для неавторизованного доступа;
- знать способы выявления ненормального поведения конкретных систем, последовательность дальнейших действий, точки контакта с ответственными лицами;
- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Abstract

The authors consider the problems of forming the policy of computer information safety.

Литература

1. Галатенко В. Информационная безопасность. Jet Info, 1996, – № 1–3.
2. Научная сессия МИФИ-2003. X всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. М.: МИФИ, 2003. – 256 с.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. Москва, 1992
4. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва. Единая Европа, 1994

Гомельский государственный
университет им.Ф.Скорины

Поступило 06.04.03