Известия Гомельского государственного университета
имени Ф. Скорины, №5(50), Ч1, 2008

УДК 681.3

Информационная безопасность и Интернет

А. Б. Демуськов, В. Л. Мережа, Г. И. Большакова, Т. П. Бышик, Т. Я. Каморникова

Уязвимость информации, обрабатываемой с помощью ЭВМ, резко увеличилась, когда в конце 80-х годов прошлого века появилось большое число вычислительных машин, открытых для доступа по телефонным линиям и другим каналам связи [1]. Быстрыми темпами растёт количество объединяемых в различного рода сети персональных компьютеров, лавинообразно увеличивается число абонентов глобальной сети Интернет. Всё это приводит к существенному расширению инструментария для потенциальных нарушителей целостности информации. Большинство нарушений, как показывает отечественный и зарубежный опыт, связано именно с проникновением в компьютерные сети. В то же время необходимость в контролируемом использовании данных (защита авторских прав, персональных данных, коммерческой тайны, сохранения секретов) растёт, что обостряет потребность как в программных и аппаратных средствах защиты, так и в организационном обеспечении функционирования сетей, а также и в правовом регулировании информационной сферы в целом [2].

Хотя подключение к Интернету и предоставляет огромные выгоды из-за доступа к колоссальному объему информации, оно же является опасным для сайтов с низким уровнем безопасности. Интернет страдает от серьезных проблем с безопасностью, которые, если их игнорировать, могут привести к катастрофе для неподготовленных сайтов. Ошибки при проектировании TCP/IP, сложность администрирования рабочих станций, уязвимые места в программах, и ряд других факторов в совокупности делают незащищенные сайты уязвимыми к действиям злоумышленников.

И чтобы правильно учесть возможные последствия подключения к Интернету в области безопасности, любая организация должна ответить себе на некоторые вопросы:

- могут ли хакеры разрушить внутренние системы?
- может ли быть изменена или прочитана важная информация организации при ее передаче по Интернету?
- можно ли помешать работе организации?

На данный момент существует много технических решений для борьбы с основными проблемами безопасности Интернета. И все они имеют свою цену. Многие решения ограничивают функциональность ради увеличения безопасности. Другие требуют идти на значительные компромиссы в отношении легкости использования Интернета. Третьи требуют вложения значительных ресурсов: рабочего времени для внедрения и поддержания безопасности; денег для покупки и сопровождения оборудования и программ.

Цель политики безопасности для Интернета – принять решение о том, как организация собирается защищаться. Такая политика обычно состоит из двух частей: общих принципов; конкретных правил работы. Общие принципы определяют подход к безопасности в Интернете. Правила же определяют, что разрешено, а что – запрещено. Правила могут дополняться конкретными процедурами и различными руководствами.

Чтобы политика для Интернета была эффективной, разработчики политики должны понимать смысл компромиссов, на которые им надо будет пойти. Эта политика также не должна противоречить другим руководящим документам организации.

Интернет – это важный ресурс, который изменил стиль деятельности многих людей и организаций. И вместе с тем, Интернет страдает от серьезных и широко распространенных проблем с безопасностью. Много организаций было атаковано или зондировано злоумышленниками, в результате чего они понесли большие финансовые потери и утратили свой престиж. В некоторых случаях организации были вынуждены временно отключиться от Интер-

нета и потратили значительные средства на устранение проблем с конфигурациями рабочих станций и сетей. Сайты, которые игнорируют эти проблемы, подвергают себя риску сетевой атаки злоумышленниками. Даже те сайты, которые внедрили у себя меры по обеспечению безопасности, подвергаются тем же опасностям из-за появления новых уязвимых мест в сетевых программах и грамотной настойчивости некоторых злоумышленников.

Основная проблема состоит в том, что Интернет при проектировании и не задумывался как защищенная сеть. Некоторыми его проблемами в текущей версии TCP/IP являются:

- легкость перехвата данных и фальсификации адресов машин в сети. Основная часть трафика Интернета – это нешифрованные данные. Электронная почта, пароли и файлы могут быть перехвачены, используя легко доступные программы;
- уязвимость средств TCP/IP. Часть средств TCP/IP была спроектирована без защиты и может быть доступна квалифицированному злоумышленнику;
- средства, используемые для тестирования, особенно уязвимы;
- отсутствие политики. Многие сайты по незнанию сконфигурированы таким образом, что предоставляют широкий доступ к себе со стороны Интернета, не учитывая возможность злоупотребления этим доступом, многие сайты разрешают работу большего числа сервисов TCP/IP, чем им требуется для работы, и не пытаются ограничить доступ к информации о своих компьютерах, которая может помочь злоумышленникам;
- сложность конфигурирования. Средства управления доступом рабочих станций сложны, зачастую сложно правильно сконфигурировать и проверить эффективность установок. Средства, которые по ошибке неправильно сконфигурированы, могут привести к неавторизованному доступу.

На сегодняшний день сформулированы три базовых принципа, которые должна обеспечивать информационная безопасность [3,4]:

- целостность данных – защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Степень доверия, или надежность систем, можно оценивать по двум основным критериям: политика безопасности; гарантированность [5].

Для того, чтобы описать политику по данной области, администраторы сначала должны определить саму область с помощью ограничений и условий в понятных всем терминах. Часто также полезно явно указать цель или причины разработки политики – это может помочь добиться соблюдения политики. В отношении политики безопасности в Интернете организации может понадобиться уточнение, охватывает ли эта политика все соединения, через которые ведется работа с Интернетом или собственно соединения Интернет. Эта политика также может определять, учитываются ли другие аспекты работы в Интернете, не имеющие отношения к безопасности, такие как персональное использование соединений с Интернетом.

Как только предмет политики описан, даны определения основных понятий и рассмотрены условия применения политики, надо в явной форме описать позицию организации (то есть решение ее руководства) по данному вопросу. Это может быть утверждение о разрешении или запрете пользоваться Интернетом и при каких условиях.

Проблемные политики требуют включения в них описания применимости. Это означает, что надо уточнить, где, как, когда, кем и к чему применяется данная политика.

Нужно описать ответственных должностных лиц и их обязанности в отношении разработки и внедрения различных аспектов политики. Для такого сложного вопроса, как безопасность в Интернете, организации может потребоваться ввести ответственных за анализ безопасности различных архитектур или за утверждение использования какой либо архитектуры.

Для некоторых видов политик Интернета может оказаться уместным описание, с некоторой степенью детальности, нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно описаны наказания, и это должно быть 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.

Интернет – это только один из множества способов, которыми организация обычно взаимодействует с внешними источниками информации. Политика Интернета должна быть согласована с другими политиками в отношении взаимоотношений с внешним миром.

Интернет 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. Многие сотрудники не понимают общественный характер Интернета.

Интернет – это не единственная глобальная сеть. Организации используют телефонные сети и другие глобальные сети для организации доступа удаленных пользователей к своим внутренним системам. При соединении с Интернетом и телефонной сетью существуют аналогичные угрозы и уязвимые места.

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. А учитывая возможности Вузов основы информационной безопасности должны быть даны студентам уже на первом курсе, независимо от получаемой специальности.

Политики компьютерной безопасности должны доводиться таким образом, чтобы гарантировалась поддержка со стороны руководителей отделов, 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 работ.

В настоящее время выделение финансовых и человеческих ресурсов на обеспечение безопасности ограничено, и требуется показать прибыль от вложений в них. Инвестиции в информационную безопасность могут рассматриваться как инвестиции для увеличения прибыли путем уменьшения административных затрат на ее поддержание или для защиты от потери прибыли путем предотвращения потенциальных затрат в случае негативных коммерческих последствий. В любом случае стоимость средств обеспечения безопасности должна соответствовать риску и прибыли для той среды, в которой работает организация.

Говоря простым языком, риск – это ситуация, когда угроза использует уязвимое место для нанесения вреда вашей системе. Политика безопасности обеспечивает основу для внедрения средств обеспечения безопасности путем уменьшения числа уязвимых мест и как следствие уменьшает риск. Типичными угрозами в среде Интернета являются [6]:

- сбой в работе одной из компонент сети – сбой из-за ошибок при проектировании или ошибок оборудования или программ может привести к отказу в обслуживании или компрометации безопасности из-за неправильного функционирования одной из компонент сети. Выход из строя брандмауэра или ложные отказы в авторизации серверами аутентификации являются примерами сбоев, которые оказывают влияние на безопасность;
- сканирование информации – неавторизованный просмотр критической информации злоумышленниками или авторизованными пользователями может происходить, используя различные механизмы – электронное письмо с неверным адресатом, распечатка принтера,

неправильно сконфигурированные списки управления доступом, совместное использование несколькими людьми одного идентификатора и т.д.;

• использование информации не по назначению – использование информации для целей отличных от авторизованных, может привести к отказу в обслуживании, излишним затратам и потере репутации. Виновниками этого могут быть как внутренние, так и внешние пользователи;

• неавторизованное удаление, модификация или раскрытие информации – специальное искажение информационных ценностей, которое может привести к потере целостности или конфиденциальности информации;

• проникновение – атака неавторизованных людей или систем, которая может привести к отказу в обслуживании или значительным затратам на восстановление после инцидента.

• маскарад – попытки замаскироваться под авторизованного пользователя для кражи сервисов или информации, или для инициации финансовых транзакций, которые приведут к финансовым потерям или проблемам для организации.

Наличие угрозы необязательно означает, что она нанесет вред. Чтобы стать риском, угроза должна использовать уязвимое место в средствах обеспечения безопасности системы и система должна быть видима из внешнего мира. Видимость системы – это мера как интереса злоумышленников к этой системе, так и количества информации, доступной для общего пользования на этой системе.

Так как многие угрозы, основанные на Интернете, являются вероятностными по своей природе, уровень видимости организации напрямую определяет вероятность того, что враждебные агенты будут пытаться нанести вред с помощью той или иной угрозы. В Интернете любопытные студенты, подростки-вандалы, криминальные элементы, промышленные шпионы могут являться носителями угрозы. По мере того, как использование глобальных сетей для электронной коммерции и критических задач увеличивается, число атак криминальных элементов и шпионов будет увеличиваться.

Организации по-разному уязвимы к риску. Политики безопасности должны отражать уязвимость конкретной организации к различным типам инцидентов с безопасностью и делать приоритетными инвестиции в области наибольшей уязвимости.

Имеется два фактора, определяющих уязвимость организации. Первый фактор – последствия инцидента с безопасностью. Почти все организации уязвимы к финансовым потерям – устранение последствий инцидентов с безопасностью может потребовать значительных вложений, даже если пострадали некритические сервисы. Тем не менее, средства переноса риска (страховка) могут гарантировать, что даже финансовые потери не приведут к кризису организации.

Одним из важных шагов при определении возможных последствий является ведение реестра информационных ценностей. Хотя это и кажется простым, поддержание точного списка систем, сетей, компьютеров и баз данных, использующихся в организации, является сложной задачей. Организации должны объединить этот список с результатами работ по классификации данных, в ходе которых информация, хранимая в онлайновом режиме, классифицируется по степени важности для выполнения организацией своих задач.

Более серьезные последствия возникают, когда нарушается внутренняя работа организации, что приводит к убыткам из-за упущенных возможностей, потерь рабочего времени и усилий по восстановлению работы. Самые серьезные последствия – это когда затрагиваются внешние функции, такие как доставка продукции, потребителям или прием заказов. Эти последствия инцидента с безопасностью напрямую вызывают финансовые убытки из-за нарушения работы служб или из-за потенциальной потери доверия клиентов в будущем.

Второй фактор – это учет политических или организационных последствий. В некоторых корпорациях верхний уровень руководства организацией может подумать, прочитав статью в известной газете о проникновении в их сеть, что произошла катастрофа, даже если при этом организация не понесла никаких финансовых убытков. В более открытых средах, таких

как университеты или научные центры, руководство может на основании инцидента принять решение о введении ограничений на доступ. Эти факторы надо учитывать при определении уязвимости организации к инцидентам с безопасностью.

И в заключение, именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает первостепенного внимания. Для поддержания режима информационной безопасности особенно важны и программно-технические меры, поскольку основная угроза компьютерным системам исходит от самих этих систем (сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.).

Стандарты и прилагаемые к ним рекомендации образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности. В то же время, эти документы ориентированы в первую очередь на производителей и "оценщиков" систем и в гораздо меньшей степени – на потребителей (пользователей). Информационную безопасность нельзя купить, ее приходится каждодневно поддерживать, взаимодействуя при этом не только и не столько с компьютерами, сколько с людьми. Иными словами, стандарты и рекомендации не дают ответов на два главных (с практической точки зрения) вопроса:

- как приобретать (комплектовать) информационную систему масштаба предприятия, чтобы ее можно было сделать безопасной?
- как практически сформировать режим безопасности и поддерживать его в условиях постоянно меняющегося окружения и структуры самой системы?

Таким образом, стандарты и рекомендации являются лишь отправной точкой на длинном и сложном пути защиты информационных систем организаций. С практической точки зрения важны рекомендации, по возможности простые, следование которым дает пусть не оптимальное, но достаточно хорошее решение задачи обеспечения информационной безопасности [4].

Abstract. The problems of computer networks in the field of information safety are presented in the paper. The principles and criteria of ensuring information safety are also considered here.

Литература

1. Герасименко, В.А. Основы защиты информации / В.А. Герасименко А.А. Малюк; Москва, 1997, МИФИ

2. Научная сессия МИФИ-2003. X всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. М:.МИФИ, 2003. 256с.

3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. Москва, 1992.

4. Демуськов, А.Б. Проблемы информационной безопасности в компьютерных сетях / А.Б.Демуськов, Г.И.Большакова, Т.П.Бышик // Известия Гомельского Госуниверситета им. Ф. Скорины, 2003. – №3 (18). – С. 124–129.

5. Демуськов, А.Б. Политики информационной безопасности предприятий / А.Б. Демуськов, В.А. Короткевич, Л.И.Короткевич // Известия Гомельского Госуниверситета им. Ф. Скорины, 2003. – №4 (19) – С. 31–36.

6. Демуськов, А.Б. Определение политики сетевого доступа / А.Б.Демуськов, В.Л. Мережа, Т.П. Бышик, Т.Я. Каморникова // Известия Гомельского Госуниверситета им. Ф. Скорины, 2007. – №5 (44).– С. 126–129.

Гомельский государственный
университет имени Ф. Скорины

Поступило 21.04.08