Безопасность по стандарту или аспирин для админа

С. А. Козлов
sergeyk@tsi.lv

11 августа 2003 г.

Аннотация

В статье произведена попытка обзора документов регламентирущих безопасность ИС и связанных с ними областями. Автор не претендует на роль эксперта по безопасности.

Статья написана в качестве контрольной работы по курсу «Безопасность компьютерных сетей» в Институте Транспорта и Связи.

1 Введение

> «Ничто так не способствует успешному внедрению новшеств, как отсутствие проверок»
>
> *Закон Муэнча [1]*

Для начала попробуем отвлечься от Информационных Технологий(ИТ) и рассмотреть простой бытовой пример: есть некоторое помещение с дверью. Некто, кто не должен был попасть в это помещение, оказался в этом помещении — кто виноват? Это помещение защищено? А если это помещение Ваш кабинет, квартира, комната или офис? У вас на каждой двери, выполненной из титана, установлен замок четвёртого класса стойкости[1]? Почему?

[1]ГОСТ 5089-97 «Замки и защелки для дверей. Технические условия.»

Безопасность сама по себе бессмысленна. Реальная Информационная Система(ИС) — это всегда компромисс между функциональностью и безопасностью, с поправкой на материальные затраты.

В быту и на малых фирмах вопросы безопасности решаются интуитивно: эмпирически, сисадмин или хозяин находит «золотую середину» в этом вопросе, а оценка производится по принципу «До первой поломки». Такой подход вполне естественен и оправдан — системный подход к безопасности может оказаться непомерной затратой. Если же убытки от простоя вычислительной техники превышают её стоимость, то есть смысл задуматься о детальном рассмотрении проблем безопасности, т.е. определиться с решаемыми задачами и оценить риски.

Вирусы, хакеры, ошибки пользователей и в Програмном и Аппаратном Обеспечении(ПО и АО) способны вызвать стрессовое состояние у любого человека связанного с компьютерами. Постоянные сообщения об обнаружении «дыр» в программном обеспечении именитых производителей могут привести в уныние любого администратора, ибо потратить всю жизнь на исправление не самая лучшая перспектива для творческой личности. Здесь, во избежание нервного расстройства, лучше воспользоваться советом именитого психолога: расслабиться и последовательно разобраться в сложившейся ситуации [2].

ПО любого производителя и на любой платформе будет иметь ошибки, ибо программы пишут, устанавливают и эксплуатируют люди, а людям свойственно ошибаться. Абсолютно надёжного ПО не существует. Так же как не существует абсолютно надёжного аппаратного обеспечения.

Применять все, рекомендуемые производителем, исправления ПО и правила и нормы безопасности весьма сложно, ибо исправляя одни ошибки, патчи могут иметь другие ошибки или особенности. Отдельные правила могут утрачивать значение с изобретением новых методов атак или вступать в противоречие с другими правилами или со здравым смыслом [3].

Если Ваш бизнес не относится к классу пресловутого «неуловимого Джо», то у Вас будут конкуренты и недоброжелатели. В любом случае следует учитывать хакеров-«альтруистов» способных взломать «всё и вся» не соизмеряя материальные затраты.

Более детально составляющие угрозы информационной безопасности рассмотрены в [4].

«Что может быть проще! Купите CoolFirewall с SuperServer и у Вас не будет проблем, а цена конечно высокая, ибо безопасность не может стоить дёшево!» — воскликнут в фирме торгующей дорогой аппаратурой и ПО для защиты. Возможно красивая коробка действительно обеспечи-

вает то что написано в рекламных проспектах, но стоит ли платить такие деньги за это? Ведь это надо обосновать и шефу. А потом обосновать, что, несмотря, на вновь возникшие проблемы, деньги были выброшены незря. Другими словами: как оценивать затраты и результат? Какую прибыль приносит безопасность? [15]

И так, разобравшись, создаётся впечатление, что задача обеспечения безопасности неразрешима. Да, это так, более того — в такой постановке[2] задача в принципе не имеет решения. Но решение есть и более того оно стандартизовано и не одно! В общих чертах для обеспечения безопасности (и, что важно, для её измерения) необходимо определиться в том: «Что и кому собираемся предоставлять или продавать?». Для частного пользователя: «Что собираюсь получить от компьютера или сети?», «Что и от чего или кого собираемся защищать?». Чем точнее будут сформулированы ответы тем легче будет построить и поддерживать и бизнес и безопасность и тем выше будет безопасность.

Ответив необходимо расставить приоритеты, а ещё лучше расставить ответы на выше приведенные вопросы в порядке приоритетности: решая в каждом конкретном случае что важнее цель или безопасность. Результатом будет основа политики безопасности.

Собственно безопасность измеряется в выполненности пунктов политики безопасности. Именно «простое» выставление «галочек» по пунктам кроется за красивой формулировкой «аудит системы безопасности»[3]. И следовательно нельзя провести аудит, т.е. нельзя оценить безопасность, там, где нет чётко сформулированной политики безопасности. И в тоже время продуманная и корректно составленная политика безопасности относительно легко претворяется в жизнь, не мешая делу, и позволяет оценивать безопасность самой себя.

Это конечно идеал, и идеал почти недостижимый, но к которому надо стремиться.

При кажущейся лёгкости построения, вышеописанной, системы безопасности и её оценке на основе политики безопасности тут есть одно большое «но»: всё упирается в составление этой самой политики безопасности, документа на который можно потратить всю жизнь и не написать ни одной строчки. . . если не обратиться к опыту других. Именно такой опыт собран в различных стандартах и рекомендациях — это и алгоритмы составления политики безопасности и шаблоны должностных инструкций и типовые структуры подразделений и т.д. и т.п.

---

[2]Точнее сказать: «в отсутствии постановки».

[3]Да простят меня профессиональные эксперты и аудиторы за столь вольную трактовку :)

2 Законодательная составляющая безопасности

Dura lex, sed lex.

Если для частного лица безопасность его домашнего компьютера только его личное дело, то для фирм это уже вопрос и юридический, ибо так или иначе большинство ИС, эксплуатируемых на фирмах занимаются обработкой личных данных сотрудников и клиентов, а эти системы попадают под законадательные акты ЕС [5] и ЛР [6, 7, 8].

К сожалению в обществе весьма популярно мнение что безопасность это сугубо техническая проблема и негоже её решать «бюрократическими методами». Невнимательность пользователя воспринимается как должное, а взломщик возводиться в ранг «благородного пирата». Такая ситуация является тупиковой и сильно напоминает ситуацию в конце XIX века вокруг «медвежатников». Тем неменее опыт борьбы с криминалом в реальном мире [14], вполне применим, наряду с административными методами, и в виртуальном мире ИТ.

3 Текущее положение

Возраст ИТ, на фоне человеческой эволюции, мизерен, но накопленный опыт в виде стандартов и рекомендаций, для отдельного человека, весьма огромен и подробно рассмотреть в рамках небольшой статьи невозможно: по каждому отдельному стандарту написаны тома пояснений, проводятся лекции и курсы по сертификации и популяризации [9, 10]. Но немного систематизировать этот опыт можно. По направленности можно выделить стандарты безопасности, библиотеки опыта и общие стандарты. Именно в таком порядке их и рассмотрим.

3.1 Стандарты безопасности

3.1.1 ISO 15408

Международный стандарт построения систем безопасности и аудита.

3.1.2 BS 7799

Британский стандарт «Управление Информационной Безопасностью». Документ «BS7799: Управление ИБ» состоит из двух частей.

В Части 1: «Практические рекомендации», 1995 г., определяются и рассматриваются следующие аспекты ИБ:

- Политика безопасности.
- Организация защиты.
- Классификация и управление информационными ресурсами.
- Управление персоналом.
- Физическая безопасность.
- Администрирование компьютерных систем и сетей.
- Управление доступом к системам.
- Разработка и сопровождение систем.
- Планирование бесперебойной работы организации.
- Проверка системы на соответствие требованиям ИБ.

Часть 2: «Спецификации системы», 1998 г., рассматривает эти же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта [16].

3.1.3 ISO 17799

Международный стандарт безопасности информационных систем и аудита.

3.1.4 BSI

Германский стандарт. В 1998 году вышло «Руководство по защите информационных технологий для базового уровня». Руководство представляло собой гипертекст объемом около 4 МБ (в формате HTML). Руководство предлагает методологию управления ИБ с подробным рассмотрением составляющих от организационного уровня ИБ до принятия контрмер с классификацией. На данный момент документ BSI и все что с ним связано доступно в Интернете [16, 17].

3.1.5 SAC, SAS 55/78

Стандарты методов аудита безопасности.

3.1.6 ITSEC

Критерий Оценки Безопасности ИТ. Принят во Франции, Германии, Нидерландах, Объединенном Королевстве. Поддерживается Европейской Комиссией (см. также TCSEC, эквивалент в США)

3.1.7 TCSEC

Критерий Оценки Надежности Компьютерной Системы, также известный как Оранжевая книга: критерий оценки компьютерных систем, впервые определенный Департаментом Безопасности (см. также ITSEC, эквивалент в Европе)

3.2 Библиотеки опыта

Собственно это не совсем стандарты, точнее совсем не стандарты. Это собрание опыта в чистом виде, т.е. коллекции образцов решений в области ИТ.

3.2.1 KNET

3.2.2 IT Infrastructure Library, ITIL, www.itil.org

Библиотека Инфраструктуры Информационных Технологий.

По рекомендациям ITIL деятельность по обеспечению сервисов представляется в виде процессов.

Процесс — это последовательность шагов, направленная на достижение определенной цели или результата.

3.3 Общие стандарты

Наиболее рациональный подход реализован в общих стандартах, в которых безопасность является только частью, связанной с основной задачей.

3.3.1 CoBit

Контрольные Объекты для Информационной и смежных Технологии — масштабная научно-исследовательская работа, результаты которой опубликованы Фондом Аудита и Контроля Информационных Систем (ISACF).

Цели создания COBIT — разработать согласованный набор международных стандартов для управления, контроля и аудита ИС, которые могут быть применены для ИС масштаба предприятия: от уровня локальных вычислительных сетей до крупных распределенных вычислительных комплексов. Проект был начат с разработки структуры контроля ИС и основан на ранее опубликованных ISACF Объектах Контроля с некоторыми изменениями и добавлениями, призванными соотнести стандарт с требованиями руководителей и в будущем соответствовать практическим потребностям аудиторов информационных систем. Это было сделано на основании критического обзора задач управления, действий направленных на реинжениринг бизнес процессов и выбор оптимальной платформы. После дополнений стандарт был согласован с действующими юридическими и фактическими стандартами и инструкциями, которые существовали во всем мире на момент его издания.

В настоящее время стандарт CoBIT создается ISACF, но продвигается и поддерживается ассоциацией ISACA переживая свое третье издание.

Утверждение, лежащее в основе CoBIT: «Ресурсы информационных систем должны управляться набором естественно сгруппированных процессов для обеспечения организации необходимой и надёжной информацией». Весь стандарт выстроен на основании этого утверждения.

3.3.2 ISO 9000

Структуры управления и соответствия качества. Общий стандарт, на прямую нерегламентирующий безопасность, но требующий детального и чёткого определения целей и задач организации, что существенно облегчает обеспечение безопасности ИС сертифицированной по ISO 9000 организации.

3.3.3 SPICE

Улучшение Процесса Программирования и Определение Производительности — структура улучшения процесса программирования.

3.3.4 TickIT

Схема сертификации систем качества для программного обеспечения.

4 Типичные заблуждения

Систему построенную по стандарту нельзя взломать. Нужно как можно быстрее написать политику безопасности и все будет в порядке. Нам нужна 100% защита, при нулевых потерях и затратах. В этом отношении очень подходит аналогия с UPS'ами: «Поставьте UPS фирмы MMM и у Вас не будет проблем с питанием!» — типичный рекламный слоган. На русский его можно перевести так: «Поставив UPS Вы, скорее всего, избавитесь от мелких проблем, а о крупных, вероятно, будете предупреждены.» Политика безопасности даёт возможность оценить и предупредить многие потенциальные проблемы, но не способна избавить от проблем полностью — безопасность оперирует вероятностями и оценивает с заданной долей вероятности. Разработка политики безопасности позволяет заранее оценить возможные убытки и соразмерить их с затратами [15]. Политика безопасности — это «незыблемый монолит» созданный раз и на всегда. Огромный потенциал ИТ и прогресс в этой области весьма динамичен. Взаимное влияние ИТ на смежные области и наоборот приводит к постоянному изменению и совершенствованию как отраслевых норм и стандартов так и в области ИТ. Фирма или предприятие является развивающимся и изменяющимся «живым организмом» для которого то что было полезно вчера бесполезно сейчас, а завтра может оказаться вредным.

5 Выводы

Совет: не слушать никаких советов, в том числе и этого.

Техника в руках дикаря — груда металла.

Немного перефразировав: стандарты под пером дикаря — куча бумаги. Политика безопасности фирмы — фактически внутренний стандарт, закон обязательный для всех. И при составлении надо учитывать человеческий фактор «в квадрате»: понимаемость и исполняемость написанного. Очевидно, что неправильно понятый и, соответственно, неверно исполненный стандарт так же будет угрозой безопасности, как и его отсутствие, с той разницей что «стрелочника» будет легче найти.

Надеюсь так же очевидно и то, что построение эффективной и безопасной ИС требует чёткого понимания проблем и методов не только персоналом ИТ подразделения, но и на всех уровнях применения ИТ и, главное, руководством фирмы или предприятия. Разговор и документирование должно вестись в коректных терминах выбранного стандарта и соответсвующих применяемых технологиях.

Список литературы

[1] А. Блох, Законы Мэрфи, http://jian.euro.ru/merphy.htm, 06.04.2003

[2] Д. Карнеги, Как преодолеть чувство беспокойства.

[3] П. Семьянов, Безопасность против безопасности, http://www.ssl.stu.neva.ru/psw/publications/secvssec.html, 06.04.2003

[4] Введение в информационную безопасность, http://emanual.ru/download/1030.html, 13.04.2003

[5] Конвенция о защите физических лиц в отношении автоматической обработки личных данных, Европейский Союз, Страсбург, 28.01.1981

[6] Правила безопасности информационных систем, Латвийская Республика, Кабинет министров, Правила № 106, Рига, 21.03.2000

[7] Закон о защите личных данных физических лиц, Латвийская Республика, Рига, 23.03.2000

[8] Обязательные технические и организационные требования к защите системы обработки личных данных, Латвийская Республика, Кабинет Министров, Правила № 40, Рига, 30.01.2001

[9] Центр Информационных Технологий, http://www.citmgu.ru

[10] Домина Секьюрити, http://www.dominasecurity.com

[11] КомпьютерПресс 3'2003 (159)

[12] COBiT

[13] The Information Systems Audit and Control Association & Foundation, http://www.isaca.org, http://www.isaca-russia.ru, 06.04.2003

[14] Ю. Торвальд, Сто лет криминалистики.

[15] Концепция безопасности — математический анализ эффективности, http://kiev-security.org.ua/box/2/130.shtml, 06.04.2003

[16] С. Симонов, Анализ рисков, управление рисками, Jet Infosystems, 2000.

[17] http://www.bsi.bund.de/gshb/english/etc/e-conten.htm, 2003