АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

Сертификация и политика безопасности

БЮРОКРАТИЯ ИЛИ ПОЛЕЗНЫЕ ЭЛЕМЕНТЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ОЧЕНЬ ШИРОКАЯ ОБЛАСТЬ ЗНАНИЙ, КОТОРАЯ ОТНЮДЬ НЕ СВОДИТСЯ К ИСКЛЮЧИТЕЛЬНО ТЕХНИЧЕСКИМ МЕРАМ ПРОТИВОДЕЙСТВИЯ. ПОНИМАТЬ УПРАВЛЕНЧЕСКО-АДМИНИСТРАТИВНЫЕ, ПРОЦЕССУАЛЬНЫЕ, ЮРИДИЧЕСКИЕ И ПРОЧИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕ МЕНЕЕ ВАЖНО, ДАЖЕ ЕСЛИ ВЫ ПРОГРАММИСТ ИЛИ СИСТЕМНЫЙ АДМИНИСТРАТОР.

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

А если вы — консультант по информационной безопасности и в ваши обязанности входит проведение аудитов безопасности и расследование компьютерных преступлений, то значимость такого понимания возрастает в разы. Многие технические меры по защите информации бессмысленны, если они не подкреплены соответствующими положениями политики безопасности, если за ними не закреплены сотрудники, несущие прямую ответственность, и если все процедуры по их внедрению и поддержке не расписаны поэтапно в соответствующих руководствах и формулярах, доступных всем, принимающим в этих процедурах участие. К примеру, как бы ни была отлажена система журналирования с технической стороны, при отсутствии документированных процедур по регулярному просмотру, анализу, архивированию и резервному копированию логов, а также официально закрепленного за осуществлением этого процесса системного администратора или другого специалиста, логи в качестве доказательств в суде не принимаются. И даже если абсолютно ясно, кто виноват в произошедшем инциденте и как все было, наказать нарушителя (по крайней мере через суд) не удастся (разве что если выбить из него чистосердечное письменное признание в содеянном методами «ректотермального криптоанализа»). А за административное наказание без юридических оснований он и сам может подать на вас в суд. И выиграть. Это лишь небольшой, частный пример проблемы, которой можно было бы избежать, имея полноценную, профессионально разработанную корпоративную или организационную политику безопасности и неукоснительно следуя ее положениям и целеуказаниям.

Однако многие до сих пор считают установленные корпоративные правила и руководства по безопасности ненужным бумажным хламом, а если и держат их, то только исключительно на полке «для галочки», а управление информационной безопасностью пускают на самотек, концентрируясь на сугубо технических средствах и скидывая контрольно-управленческую функцию на и без того перегруженных сисадминов. В то время как всем этим под строгим контролем вышестоящего руководства должен заниматься глава по информационной безопасности компании, а при отсутствии такой должности — ее ИТ-директор.

Эта проблема далеко не нова и хорошо знакома правительствам, международным организациям по стандартам и промышленным бизнес-ассоциациям. Они пытаются с ней бороться посредством введения различных общепризнанных аккредитаций по информационной безопасности, предоставляющих имеющим их компаниям выраженные конкурентные преимущества. Ибо невозможно получить или обновить ни один международный сертификат по информационной безопасности, не имея корректно составленной и регулярно проверяемой и обновляемой политики безопасности. И первое, на что смотрят пришедшие в компанию аудиторы, — это соответствие таким аккредитациям, наличие политики безопасности и проистекающих из нее документов. И только потом проверяется соблюдение изложенного на бумаге в каждодневной практике, включая различные технические аспекты. Логично, не правда ли? И если политика безопасности и связанные с ней указания, формуляры, корпоративные стандарты, руководства отсутствуют напрочь или явно неадекватны, аудиторы даже не будут смотреть на ваш самый новый, мегадорогой и под завязку набитый модулями для акселерации фильтрования и обнаружения атак гигабитный межсетевой экран. И то, как часто обновляется ваш антивирус или меняются пароли пользователей, их тоже не заинтересует.

Однако

Иногда, правда, может доходить почти до абсурда. Так, несколько месяцев назад автор статьи столкнулся с тем, что аудиторы из KPMG отметили как один из существенных недостатков компании отсутствие стандартов и указаний по написанию безопасного кода для ее программистов. На самом деле вся эта документация размещалась на корпоративном вики-сервере и просто не была распечатана и вручена каждому из программистов в отделе разработки.

С чего начать

Прежде чем проводить аудит и выходить на сертификацию, компания должна убедиться, что ее система управления информационной безопасностью отвечает всем требованиям того или иного стандарта (к примеру, ISO/IEC 27001:2005). Во-первых, осуществляется предварительное обследование компании – с целью получения необходимой информации о ней, ее информационной системе, мерах по защите и методах управления информационной безопасностью, а также для выявления несоответствий требованиям. По результатам данных работ определяются границы системы управления информационной безопасности, а также перечень работ, необходимых для создания такой системы. Далее формируется проект заявления о применимости, содержащий перечень требований, которые на текущий момент выполняются или не выполняются в компании. Так как в компании должна присутствовать единая система взглядов на вопросы обеспечения информационной безопасности, производится разработка основных нормативных документов, которые согласовываются и утверждаются руководством. К числу таких документов относятся «Политика информационной безопасности» и «Методика анализа рисков информационной безопасности».

Основные международные сертификации по информационной безопасности

Полезность от получения общепризнанных аккредитаций по информационной безопасности можно разделить на две категории: с точки зрения бизнеса и с точки зрения защиты информации.

С точки зрения бизнеса их наличие как минимум демонстрирует, что руководство компании тщательно заботится о деловой и персональной информации, с которой имеет дело, и не жалеет на ее защиту времени и ресурсов. Таким образом, это своеобразный «знак качества»: возрастает доверие к организации и улучшается ее имидж. Если компания сертифицирована по всем правилам, то ее бизнес-партнерам и клиентам нет нужды проводить какие-либо дополнительные независимые аудиты, чтобы удостовериться, что меры по защите коммерческих транзакций между ними и компанией будут приняты и что любой необходимый в процессе партнерства или оказания услуг обмен конфиденциальными данными формально оправдан.

Как максимум сертификация по информационной безопасности открывает новые рын-

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

ISO 17799

Изначально назывался BS 7799 и был разработан Британским институтом стандартов при участии ряда крупных коммерческих организаций. В 1995 году стандарт BS 7799 в качестве свода установленных норм и правил по отношению к обеспечению ИБ получил в Великобритании статус государственного.
Описывает более 120 механизмов контроля, необходимых для построения системы управления информационной безопасностью организации. Эти механизмы были разработаны на основе лучших примеров мирового опыта в данной области и подходят любой организации независимо от ее размера и направления деятельности. Стоит отметить, что сертификация по ISO 17799 не проводится – документ представляет собой лишь сборник лучших практик и является неким руководством по созданию системы обеспечения информационной безопасности организации. В какой-то мере здесь уместна аналогия ITIL, с поправкой на то, что ITIL претендует на роль стандарта де-факто для IT, а BS 7799 – для информационной безопасности.

ки и коммерческие возможности. К примеру, все без исключения организации, которые в процессе своей деятельности принимают, обрабатывают и сохраняют данные кредитных карт Visa и MasterCard, обязаны поддерживать стандарт PCI DSS. Несоответствие данному стандарту приведет в лучшем случае к крупным штрафам, а в худшем — к международному запрету компании заниматься коммерцией с использованием Visa, MasterCard и многих других кредитных карточек. Особенно строгое отношение здесь к компаниям, принимающим кредитные данные в онлайновом режиме. Существуют и аккредитации, которые, не имея непосредственного отношения к ИТ-безопасности, тем не менее ее достаточно сильно затрагивают и являются абсолютно необходимыми для ведения бизнеса в определенных сферах и/или определенных государствах.
С точки зрения защиты информации сертификация вынуждает фирмы не только разрабатывать политику безопасности и содержать имеющую к ней отношение документацию в полном порядке, но и всем этим положениям так или иначе следовать. В частности, проводить регулярные независимые аудиты безопасности и реагировать на их результаты. Согласно опыту, большинство компаний обращается за независимыми проверками соответствия нужному стандарту безопасности тогда, когда их как следует поджимает необходимость получения или подтверждения требующих этих проверок аккредитаций, а неотвратимый приход аудиторов уже маячит на горизонте. Предприятия, в которых произошел инцидент («помогите, взломали!»), идут следующими по частоте обращений. А компании, заказывающие аудиты безопасности по собственной инициативе, вследствие понимания важности тщательной проверки защиты данных, сетей и систем, увы, совсем редки и отстают от двух лидирующих категорий со значительным разрывом. И только этот отдельно взятый факт уже однозначно демонстрирует пользу необходимости получения рассматриваемых ниже аккредитаций. Невозможно пройти сертификацию, задекларировав на бумаге ту или иную меру безопасности, будь то регулярная ротация паролей пользователей, проведение аудитов, наличие централизованной системы установки заплаток или систем обнаружения несанкционированного доступа, и не воплотив ее на практике. Конечно, бывает всякое и может «повезти», но обычно аудиторы таких вещей не пропускают. Ознакомимся же вкратце с основными международными стандартами по информационной безопасности, которые могут затрагивать интересы российские компаний и организаций.

ISO 27001

Стандарт ISO 27001 (полное название — ISO/IEC 27001:2005) был опубликован в октябре 2005 года, он заменил старый BS7799-2 Британского института и стандартизации (BSI). Это спецификация для корпоративных систем управления информационной безопасностью (СУИБ), обозначающая основные требования к планированию, внедрению, управлению, мониторингу, поддержке, проверке и улучшению этой самой документированной СУИБ. Сам BS7799 просуществовал достаточно долго, будучи опубликованным еще в 1995 году как свод правил. По мере его развития возникла вторая часть свода, посвященная системам управления безопасностью. Именно по этой второй части и дается официальная аккредитация.
По сути ISO 27001 улучшил содержание BS7799-2 и гармонизировал его с другими стандартами, такими как ISO 9001 (системы управления качеством) и ISO 14001 (системы управления средами). В отличие от ISO 17799, который является общим рекомендательным документом, ISO 27001 — это формальная спецификация, состоящая из следующих глав:

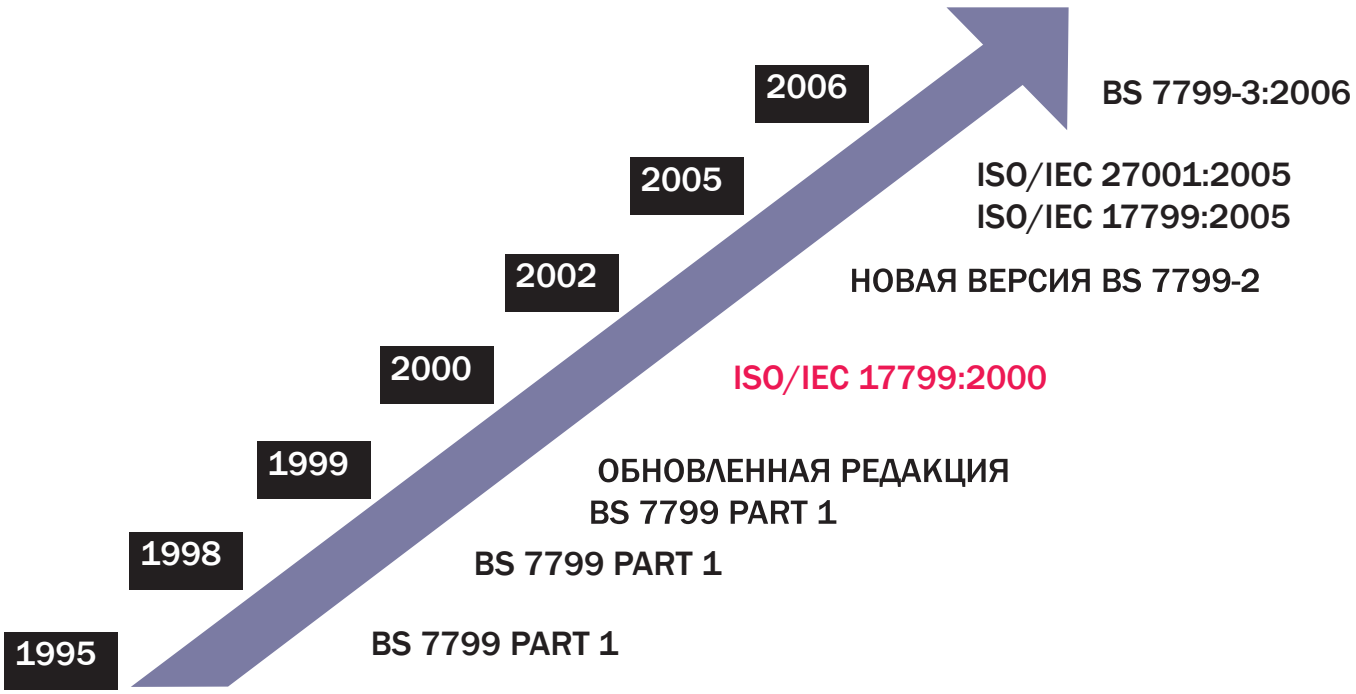
0. Введение
1. Контекст
2. Нормативные справки
3. Термины и определения
4. СУИБ
5. Ответственность руководящего персонала

ISO 27001

Более подробную англоязычную информацию по ISO 27001 и имеющим к нему отношение стандартам можно найти на следующих сайтах: www.27001-online.com и www.iso27001security.com. Особо советуем обратить внимание на раздел www.27001-online.com/secpols.htm, посвященный структуре и содержанию политики безопасности согласно ISO 27001. При составлении политики безопасности для клиентов многие стараются ориентироваться на схематику, предоставленную на указанном разделе сайта. Она не только оправдывает себя в практическом смысле, но и дает компании готовый элемент соответствия ISO 27001 и точку ссылки на истоки их политики безопасности при возникновении каких-либо вопросов о ней.
В большинстве случаев эту структуру и содержание политики безопасности, ее костяк и хребет, удается сохранить за исключением нескольких достаточно специфических разделов. Так, составляя политику безопасности для крупного инвестиционного фонда в начале этого года, автору этой статьи пришлось полностью исключить главу об электронной коммерции, использования которой нет в планах фонда даже на отдаленное будущее. Вместо нее восьмой главой стала глава о беспроводной безопасности (которая не упоминается отдельно на www.27001-online.com/secpols.htm), как более важная и уместная для фонда. Также была добавлена дополнительная подробная глава о правилах безопасного использования и технических мерах защиты систем, применяемых сотрудниками в командировках и дома для работы с информацией фонда и удаленного доступа к его сетям.

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

ПО СОСТОЯНИЮ НА АВГУСТ 2006 ГОДА В МИРЕ ЗАРЕГИСТРИРОВАНО БОЛЕЕ 2800 ОРГАНИЗАЦИЙ ИЗ 66 СТРАН, СЕРТИФИЦИРОВАННЫХ ПО ISO 27001 (BS 7799), В ИХ ЧИСЛЕ И ЧЕТЫРЕ РОССИЙСКИЕ КОМПАНИИ



6. Рецензирование СУИБ со стороны менеджеров
7. Улучшение СУИБ

Организации могут сами определять охват их инфраструктуры и операций сертификацией ISO 27001. Поэтому наличие и понимание рамочных документов (известных как «Акты по применимости») является ключевым для придачи значения этому сертификату. Если корпоративный акт по применимости ISO 27001 относится только к избранным отделам компании, то ее сертификация по ISO 27001 к другим отделам не относится и ничего об уровне их информационной безопасности не говорит. Сертификация по ISO 27001 полностью опциональна, но все больше международных компаний и иностранных правительств требуют ее наличия у своих партнеров и поставщиков. Подобно тому, как стандарты ISO 9000 говорят о том, что поддерживающие его компании и организации заботятся о качестве своей продукции и предлагаемых услуг, ISO 27001 свидетельствует о серьезном отношении к информационной безопасности и соответствии принимаемых мер защиты общепринятым международным нормам. В России первым по ISO 27001 был аккредитован «Лукойл».

Стоит еще сказать пару слов об ISO 27002:2005, в который 10 июля 2007 года был наконец-то переименован ISO 17799:2005. Как и в случае с ISO 17799:2005, формальная сертификация и аккредитация здесь отсутствуют, это фактически свод рекомендаций и советов по рычагам управления, процессам и механизмам СУБД, структура и требования к которой изложены в ISO 27001. Таким образом, соответствие ISO 27002:2005 необязательно, но содействует получению ISO 27001:2005. Кроме того, материалы и подходы ISO 27002:2005 также можно использовать для написания толковой политики безопасности (структура в данном случае мало отличается от вышеописанной для 27001) и принятия других мер по ее обеспечению. Более подробно с этим стандартом можно ознакомиться по адресу www.iso27001security.com/html/27002.html.

> МНОГИЕ ТЕХНИЧЕСКИЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ БЕССМЫСЛЕННЫ, ЕСЛИ ОНИ НЕ ПОДКРЕПЛЕНЫ СООТВЕТСТВУЮЩИМИ ПОЛОЖЕНИЯМИ ПОЛИТИКИ БЕЗОПАСНОСТИ

PCI DSS

Программа «Payment Card Industry Data Security Standard» (PCI DSS) создана для построения унифицированной полноценной системы защиты информации владельцев всех типов кредитных карт. Она является результатом кооперации между VISA и MasterCard и с 30 июня 2005 года обязательна для всех коммерческих организаций и компаний, имеющих дело с данными кредитками. Требования PCI DSS были основаны на «Программе по обеспечению безопасности данных владельцев кредитных карт» от VISA, введенных в июне 2001 года. Оценка соответствия PCI DSS основана на ряде

АВТОР: АНДРЕЙ ВЛАДИМИРОВ, CSO ARHONT LTD (WWW.ARHONT.COM)

критериев, относящихся к конфиденциальности, целостности и доступности всех обрабатываемых и хранимых данных кредитных карт. Существует 12 ключевых обобщенных требований по безопасности PCI DSS, каждое из них, в свою очередь, делится на несколько более детальных секций. Эти секции описывают методы контроля внешнего и внутреннего доступа к конфиденциальной информации на таких уровнях, как сети, коммуникационные каналы, серверы, программные приложения и политика безопасности. PCI DSS требует от компаний подробного журналирования всех фактов доступа к данным владельцев карт, ежедневной проверки этих журналов и способности реконструкции широкого круга событий, связанных с обработкой и хранением кредитной информации, с детальными логами каждого имеющего к ней отношение события. Она устанавливает, что все «торговые субъекты первого уровня» (те, через кого проходит более 6 млн. транзакций с кредитными картами в год) должны проходить ежегодный локальный аудит их систем и процедур безопасности. Этот аудит может проводиться внутренним персоналом с одобрения и под надзором директоров компании или же независимыми экспертами. Проверка независимыми экспертами рассматривается как более желательная, благонадежная и эффективная. Организации и компании 2-го (1–6 млн. транзакций в год) и 3-го (от 20 000 до 1 млн. транзакций в год) уровней не обязаны проводить ежегодный локальный аудит. Тем не менее многие из них все равно нанимают независимых консультантов для проверки на соответствие требованиям PCI DSS во избежание возможных проблем с предоставляющими кредитные сервисы компаниями и банками (VISA, MasterCard и т. д.).

Соответствие PCI DSS достигается путем внедрения совокупности процедур, процессов и технических мер противодействия злоумышленникам. Несмотря на активный маркетинг ряда продуктов, таких как системы предупреждения вторжения, с упоминанием их необходимости для PCI DSS, помните, что ни один производитель не может предложить универсального решения, гарантирующего соответствие требованиям этого стандарта после установки и конфигурации! В лучшем случае они могут предоставить системы, следующие рекомендациям PCI DSS, использующие описанные в программе методы технического контроля и позволяющие компании оценить свою готовность к аккредитации на соответствие требованиям стандарта.

Sarbanes-Oxley Act, FSA и Basel II Accord

В связи с ограниченным размером статьи мы можем только коснуться важных аккредитаций, которые принадлежат к сфере финансовых аудитов и отчетности и затрагивают ИТ-безопасность сертифицируемых компаний. Дело в том, что процесс финансовой (и не только) отчетности современной компании очень сильно зависит от ее информационных систем, сохраняющих и обрабатывающих бухгалтерскую информацию, и любое вторжение, особенно предумышленное и совершенное изнутри компании заинтересованными лицами может свести ценность и аккуратность отчетности к нулю.

Первым рассмотрим акт Сарбэйнса — Оксли от 2002 года (Sarbanes-Oxley Act или просто SOX), соответствие которому является необходимым для многих, особенно финансовых компаний, имеющих бизнес с партнерами в США. SOX — это федеральный закон США, принятый в качестве реакции на известные скандалы с такими корпорациями, как Enron и WorldCom. SOX охватывает такие области, как независимость аудиторов, корпоративное управление и прозрачность финансовых операций. В рамках SOX ИТ-безопасность затронута в «Интегрированной системе управления корпоративными рисками», опубликованной в 2004 году комитетом под названием COSO (Committee of Sponsoring Organizations of the Treadway Commission) и состоящей из восьми секций: внутренняя рабочая среда, постановка целей, идентификация событий, оценка риска, ответы на риски, контрольные действия, информация и коммуникации, мониторинг. Основной опор здесь делается на оценку риска информационной безопасности (включает в себя внутренние и независимые аудиты ИТ-безопасности и их формальную отчетность) и системы журналирования (особенно в плане сохранения целостности, корректной маркировки и резервного копирования учетных записей в компании).

Британским эквивалентом SOX является аккредитация FSA (Financial Services Authority), секция A5 которой посвящена контролю над ИТ-системами, охватывая все основные пункты от управления и политики безопасности до проведения регулярных независимых аудитов безопасности, использования криптографических мер защиты, методов аутентификации, силы паролей и процессов реагирования на инциденты, включая взлом. Аккредитация FSA необходима для всех финансовых компаний, ведущих бизнес в Соединенном Королевстве.

И упомянем так называемое Соглашение Базель II (Basel II Accord, «The New Accord», полное официальное название — International Convergence of Capital Measurement and Capital Standards — A Revised Framework). Базель II представляет собой требования и рекомендации Базельского комитета по надзору за банками (Basel Committee on Banking Supervision или BCBS), включающие в себя требования по ИТ-безопасности, во многом аналогичные SOX и сконцентрированные на оценке риска и мер противодействия рискам, а также сохранению корректной, целостной отчетности, включая учетные записи всех вовлеченных систем. В то время как SOX специфичен для США и бизнеса с США, отраслевая аккредитация по Базель II относится к банкам и финансовым организациям во всем мире.

Заключение

Разрабатывая политику безопасности компании или организации и согласованные с ней технические и административные меры ее обеспечения, всегда принимайте во внимание, каким международным, отраслевым или государственным стандартам так или иначе придется соответствовать. Например, если компания собирается вести международные финансовые операции, подумайте о Базель II, в США — еще и о SOX, в Великобритании — о FSA. Компании, имеющие дело с американским здравоохранением, обязаны соответствовать неописанной в статье HIPAA. Бизнес-партнеры, клиенты и иностранные правительства могут всегда затребовать аккредитации по ISO 27001, а если в бизнес вовлечены кредитные карточки, никак не отвертеться от PCI DSS. Воплощать необходимые процессы, системы и документацию согласно требованиям нужных стандартов с самого начала гораздо эффективнее, легче и дешевле, чем переделывать и переписывать все тогда, когда окажется, что от аккредитации никак не уйти. it

SOX, FSA, Базель II

- www.sarbanes-oxley.com
- www.theregister.co.uk/2005/05/03/sarbanes_oxley_for_it_security/
- www.sec.gov/spotlight/sarbanes-oxley.htm
- www.basel-ii-accord.com
- www.bis.org/publ/bcbsca.htm
- www.bis.org/publ/bcbs107.htm
- www.bis.org/publ/bcbs118.htm