

Практическое применение ISO 27001

МАКСИМ НЕЧАЕВ

ИНФОРМАЦИЯ ДАВНО ПРЕВРАТИЛАСЯ в товар, спрос на который постоянно растёт. Утрата конфиденциальной информации приносит организации прямые финансовые потери независимо от рода деятельности.

ЭКСПЕРТИЗА Неспособность организации обеспечить правильное функционирование системы защиты информации косвенным образом влияет на репутацию организации и, как следствие, ставит под угрозу само существование компании на рынке. В связи с этим растёт необходимость в создании работоспособной системы, которая бы смогла обеспечить адекватную защиту информационных активов организации.

Для решения задач этой направленности предназначен ISO/IEC 27001:2005 — международный стандарт по информационной безопасности, который ориентирован на все типы организаций независимо от размеров и рода деятельности. Одним из важных требований стандарта является отсутствие разногласий с действующим законодательством государства, в котором работает компания, — т.е. стандарт не создает причин для конфликтов на юридическом уровне.

ISO/IEC 27001:2005 определяет требования к созданию, управлению, поддержанию, мониторингу, контролю и улучшению системы менеджмента информационной безопасности (СМИБ). В свою очередь СМИБ представляет собой часть общей системы управления, основанную на оценках бизнес-рисков. Под информационной безопасностью подразумевается сохранение конфиденциальности, целостности, доступности, а также других свойств информации.

СМИБ в соответствии со стандартом является циклическим процессом, основывающимся на модели PDPC (рис. 1): Планируй (создание СМИБ) — Делай (внедрение и управление СМИБ) — Проверяй (мониторинг и контроль СМИБ) — Действуй (обновление и улучшение СМИБ).

Один из необходимых этапов создания СМИБ в организации — внедрение мер контроля и управления рисками. Перечень этих мер приведен в Приложении А к стандарту, детальное описание — в тексте стандарта ISO/IEC 17799:2005 «Информационные технологии — Методы защиты — Практическое руководство для управления системой защиты информации».

Важной особенностью стандарта является то, что СМИБ может охватывать не всю организацию, а только определённую область деятельности, критичную для данной организации, которую выбирает сама организация. По мере возникновения потребности организация может подключать и другие области деятельности, т.е. расширять область действия стандарта.

После выполнения всех необходимых этапов создания СМИБ организация обязана пройти сертификацию — подтвердить правильность построения и работоспособность СМИБ.

Получение сертификата о соответствии СМИБ организации требованиям данного стандарта предоставляет самой организации ряд существенных преимуществ:

- Повышение управляемости и надёжности.
- Повышение доверия к организации со стороны потенциальных партнёров и клиентов.
- Подтверждение прозрачности управления и системы в целом.
- Упрощение процедуры выхода на внешние рынки.
- Повышение авторитета организации как на внутреннем, так и на внешнем рынке.
- Минимизация вероятности понести убытки вследствие потери информации или одного из ее свойств (конфиденциальности, целостности, доступности).
- Гарантия выбора адекватных мер по защите информации, а значит, целесообразное использование средств, выделяемых на информационную безопасность.
- Анализ рисков информационной безопасности, который дает возможность уменьшать существующие угрозы для ресурсов организации, а также эффективно противодействовать возникновению новых.

Внедрение стандарта представляет естественный шаг для развития организации в целом. В то же время отсутствие сертифицированной СМИБ наносит ущерб организации и может привести к нежелательным последствиям, таким как:

- финансовые потери вследствие неконтролируемого распространения конфиденциальных данных;
- потеря позиций на рынке вследствие нанесения конкурирующей организацией атак по незащищённым уязвимым местам;
- ухудшение имиджа организации;
- незащищённость информационных систем от внешних атак.

Построение СМИБ в организации

Корректное построение СМИБ в организации — основа для дальнейшей деятельности организации. Специалисты организации могут разработать и внедрить СМИБ самостоятельно, выполняя требования стандарта и учитывая мировую практику, либо прибегнуть к помощи компетентных организаций, имеющих опыт в данной области. В любом случае построение СМИБ организации подразумевает прохождение следующих основных этапов.

- Предварительный аудит.

- Определение области действия и границ СМИБ.

• Назначение сотрудников, ответственных за СМИБ (создание структуры, которая будет внедрять и обеспечивать работоспособность СМИБ организации, к примеру, отдел внутренней безопасности).

- Инвентаризация активов организации и определение их важности.

• Оценка защищённости активов организации (анализ существующих угроз и уязвимостей, а также вероятностей их реализации).

• Определение подхода организации к оценке рисков (стандарт не устанавливает обязательного метода к определённому методу оценки рисков — наоборот, организация может предложить свой метод оценки рисков, и чем проще будет этот метод, тем лучше).

• Подсчёт рисков в организации как в качественных, так и в количественных показателях.

• Анализ рисков и принятие решений по обработке рисков (принять риск, уменьшить риск до допустимого уровня, передать третьей стороне, избежать риска).

• Выбор целей управления и средств для обработки рисков.

• Анализ существующих контрмер (организационные мероприятия и программно-технические средства, направленные на защиту определённого актива организации).

• Анализ процессной документации организации (создаётся список организационных документов, требующих внедрения).

Создание политики информационной безопасности (пересматриваемый до-

кумент, который должен быть одобрен руководством и представлен для изучения всем сотрудникам организации; описывает функциональные обязанности руководства и подход к управлению информационной безопасностью).

Создание Заявления о применимости (обязательный документ, который содержит все рекомендации Приложения А стандарта ISO/IEC 27001:2005 с описанием, выполняются ли данные требования в организации).

• Разработка документации СМИБ (инструкции, процедуры, методики, записи, корпоративные стандарты и т.д.).

• Внедрение СМИБ (внедрение необходимых технических средств, подготовка к аудиту и т.д.).

• Обучение персонала (проводится при принятии на работу, при внедрении СМИБ и при внесении изменений в СМИБ).

• Проведение внутреннего аудита СМИБ организации.

Но что делать, если в организации уже существует своя система информационной безопасности и строить с нуля новую представляется нецелесообразным? Выход из данной ситуации — проведение внутреннего аудита. На основе результатов такого анализа можно откорректировать действующую систему, разработать недостающие процессные документы, улучшить подход к оценке рисков в организации и т.д.

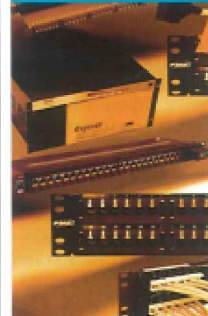
Сертификация СМИБ

Подготовкой к прохождению сертификации может заниматься как сама организация, так и организация-посредник, накопившая компетенцию в этой области. Перед началом сертификации компания должна пройти предварительный аудит, который даст возможность оце-

ПРОДОЛЖЕНИЕ НА С. 29 ►



AMP NETCONNECT - РЕШЕНИЕ ПО УПРАВЛЕНИЮ ИНФРАСТРУКТУРОЙ



Интеллектуальная AMPTRAC™ система упорядочит хаос

- Минимизация простых сетей
- Отслеживание и документирование изменений в СКС в реальном времени
- Оптимизация использования ИТ инфраструктуры
- Уменьшение эксплуатационных расходов

Животный мир демонстрирует нам как интеллектуальные идеи могут привести к функционированию "сети" в природе. В информационном мире сети становятся более прозрачными и понятными с помощью системы управления инфраструктурой AMPTRAC, где каждое коммутируемое соединение постоянно контролируется, все изменения в сети немедленно регистрируются и документируются в режиме реального времени. Система AMPTRAC — полностью автоматизированное решение с аппаратными и программными обеспечениями для новых и существующих сетей. Эксплуатация сетей — это сложный процесс. С системой AMPTRAC — логика интеллектуальная и эффективная.

Кто сказал, что нам нечему учиться у животных?



Таблица 1. ISO/IEC 27001:2005

Страна	Название	Номер сертификата	Сертифицирующий орган
Германия	Vodafone Telecommerce GmbH Ratingen	IS 58084	BSI
	Siemens Business Solutions	IS 61545	BSI
Испания	Ericsson EBPV A S.A.	IS 68816	BSI
Великобритания	Kensington Mortgage Co	IS 61291	BSI
	7 Global	IS 67048	BSI
США	Dental Practice	IS 86140	BSI
	The University Of Texas Richardson	IS 53841	BSI
Индия	Federal Reserve Bank of New York	IS 18808	BSI
	EDS Enterprise Services GSOC	IS 77016	BSI
Япония	Siemens Shared Services	Bangalore	STDC
	Polaris Software Lab Ltd.	Chennai	STDC
Австралия	Japan Trusted Systems Laboratory	IS 71437	BSI
Корея	Macquarie Corporation	IS 61344	BSI
	LG Card Co. Ltd.	IS 73879	BSI
	Samsung Life Insurance Co. Ltd.	IS 75677	BSI
	Samsung Electronics Co. Ltd. (64 sites)	IS 69872	BSI

Дистрибуторы в Украине:

ОАО «БАНКОВСВЯЗЬ»
04069, г. Киев, ул. Стрелецкая, 69
Тел.: +38 (044) 490-00-90
факс: +38 (044) 267-64-34
info@netconnect.com.ua
http://www.netconnect.ua

ИП МАКС
01033, Киев,
ул. Житомирская, 29
Тел.: +38 (044) 492-88-82
факс: +38 (044) 297-35-88
max@netconnect.com.ua
http://www.netconnect.ua

Дилеры в Украине:
NetLine, Киев,
Тел.: +38 (044) 451-79-79
Антарес, Тернополь, Киев,
Тел.: +38 (041) 664-00-04
АМИ, Львов,
Тел.: +38 (062) 385-48-88

Представительство
Tyco Electronics AMP GmbH
в Украине:
04050, г. Киев,
ул. Пилипенко, 13,
кв.10, Т/Б 11
Тел.: +38 (044) 206-22-65
факс: +38 (044) 206-22-64

кам и подрядчикам федеральных правительственных органов использовать смарт-карты для физического и логического доступа. По данным компании IMS Research, эта инициатива способна обеспечить рост рынка до 925,1 млн долл. к 2011 году. Актуальная информация и новости об унифицированной безопасности аккумулируются на сайте OSE <http://www.opensecurityexchange.org>.

Подытоживая сказанное, можно уверенно заявить, что мы находимся в начале интересной эпохи становления унифицированной безопасности как отдельного

рыночного сегмента. Он должен не просто объединить физическую и ИТ-безопасность, но и предоставить качественно новые услуги для конечных потребителей при существенном уменьшении расходов на внедрение и поддержку системы в целом. Ближайшие несколько лет должны показать, насколько оптимистичными будут эти прогнозы. □

С Владимиром Илизмаком, экспертом компании Cisco Systems, можно связаться по адресу vailizma@cisco.com

Практическое...

◀ продолжение со с. 25

нить, насколько организация готова к сертификации.

- Сертификацию может проходить СМИБ компании, которая уже проработала определенное время - не менее трёх месяцев после внедрения. Это — минимальный период, необходимый для формирования различного рода записей, анализа функционирования и т. д.

- Этап сертификации состоит из следующих шагов:

- Выбор сертифицирующего органа.
- Заполнение заявки на прохождение сертификации.

- Прохождение сертификации.

Проверка СМИБ аудитором сертифицирующего органа включает стадию проверки наличия документации — политик, процедур, методик и других документов, описывающих действия в рамках СМИБ. Проверяется наличие базы рисков информационной безопасности, методики оценки рисков, прогнозирования и управления рисками для уменьшения вероятности их возникновения и реализации. Проводится опрос персонала организации и проверка выполнения требований процессных документов СМИБ. После окончания аудита выполняются корректирующие действия по недостаткам, обнаруженным во время проверки.

Аудиты

Проведение аудитов является обязательным требованием стандарта ISO 27001. Сущность аудита на соответствие СМИБ требованиям стандарта заключается в проверке выполнения каждого положения стандарта. По каждому такому положению проверяющие должны ответить на вопросы: выполняется ли данное требование, если нет, то каковы причины невыполнения? По результатам аудита составляются отчеты, в которых фиксируются обнаруженные несоответствия. Задача организации после аудита — внедрить корректирующие действия,

МИРОВАЯ ПРАКТИКА

Стандарт ISO/IEC 27001:2005 приобрёл большую популярность в мире, о чём говорит, в частности, количество выданных сертификатов — 3890 (2007 год). В частности, сертификат получили следующие организации с мировым именем:

Показательно, что первое место по числу организаций, сертифицированных по ISO/IEC 27001:2005, занимает Япония, где правительство ввело обязательную сертификацию по этому стандарту для организаций, осуществляющих государственные поставки или участвующих в государственных тендерах. Организации стран СНГ также начали активно реализовывать требования ISO/IEC 27001:2005, что доказывает не только необходимость создания сертифицированной СМИБ, но и подтверждает значимость и эффективность самого стандарта. Ведь для организации получение сертификата означает повышение репутации и доверия клиентов, а следовательно, устойчивость на рынке и рост доходов.

направленные на устранение обнаруженных несоответствий.

По характеру аудиты разделяют на внутренние и внешние. Внутренние аудиты проводятся через запланированные организацией промежутки времени в соответствии с составленной программой. Внутренние аудиты осуществляют специалисты, сертифицированные как внутренние аудиторы, из числа сотрудников организаций-посредников, предоставляющих услуги по проведению внутренних аудитов.

Внешние аудиты проводятся сертифицирующим органом и делятся на:

- надзорные аудиты (раз в год);
- ресертификационные аудиты (раз в три года). □

С автором статьи, Максимом Нечевым, руководителем отдела технической и криптографической защиты ООО «Арт-мастер», можно связаться по адресу m_nechev@art-sof.ua

HP ProCurve...

◀ продолжение со с. 24

Защита от внутрисетевых атак

Основное средство решения проблем, связанных с различными внутрисетевыми угрозами, это системы IPS. Однако соотношение цена/производительность не позволяет гибко использовать их в современных сетях (стоимость — от 30 тыс. долл.). К тому же производители IPS, как правило, предлагают ставить их на backbone-соединениях, с 1-гигабитной, 10-гигабитной пропускной способностью.

Подход HP более гибкий: плагин Network Immunity Manager для ProCurve Manager Plus. Он реализует две основных задачи: позволяет администратору вести мониторинг трафика, проходящего через сеть, а также реагировать на его аномальности.

В модуле используются две стандартные технологии: протокол sFlow (подробнее см. врезку) и NBAD (тех-

нология обнаружения аномального поведения в сети). Основываясь на полученной из анализа трафика информации, возможно блокирование определенных MAC-адресов, IP-адресов, портов, с которых исходит сетевая угроза. Либо зеркалирование вызвавшего проблемы потока на устройство типа IPS, содержащее сигнатуры для точного определения характера угрозы.

Такой подход себя оправдывает, ведь для сети важно обнаружить «ненормальность» и заблокировать ее, а уже потом выяснять причины проблемы. Главное — обеспечить работоспособность сети. Особенность Network Immunity Manager состоит еще и в том, что он может обнаружить вирусы, которые еще, по сути, официально «не существуют», за счет выявления их симптоматики и организовать передачу вызвавшего подозрение трафика на устройства типа IPS, занимающиеся непосредственным распознаванием угрозы и ее устранением. □

Тестовая лаборатория конкурентов



Компания Telco продает
ТОЛЬКО НАДЕЖНОЕ ОБОРУДОВАНИЕ

TELCO

Официальный дистрибьютор компании
Juniper Networks и Extreme Networks в Украине

Украина, Киев, ул. Котельникова, 17, офис 81а
Телефон: +38 044 569-43-43
www.telco.ua