

Информационная безопасность.

Актуальные вопросы построения систем менеджмента с учетом требований международных стандартов информационной безопасности.

*Илья Лившиц, старший эксперт «Ассоциации по сертификации «Русский Регистр»
Руководитель направления «Системы менеджмента информационной безопасности ISO/IEC 27001:2005»
ведущий аудитор ISO/IEC 27001:2005, ISO/IEC 20000:2005;*

*Наталья Селиверстова, эксперт «Ассоциации по сертификации «Русский Регистр»
аудитор ISO/IEC 27001:2005, ISO/IEC 20000:2005*

Марцынковский Дмитрий Александрович

Исполнительный директор ООО «Русский Регистр – Международная сертификация»

Что такое информационная безопасность

Текущий экономический кризис показал, что стабильность бизнеса и экономики в целом во многом зависит от темпов развития стратегических компьютерных технологий, практики использования электронных систем и реализации аспектов информационной безопасности (ИБ).

Успешная деятельность организации зависит не только от продуманной стратегии, умения просчитывать рыночную ситуацию и лояльного коллектива, но и от ряда существенных и не всегда очевидных факторов, влияющих на устойчивость бизнеса. Один из таких факторов - обеспечение ИБ. Достаточно много говорится о том, что наш век – век информационных технологий (ИТ), что объем перерабатываемых документов в мире за год составляет астрономическое число (по данным IDC объем всей цифровой информации, созданной человечеством в 2009 году составил 161 экзбайт (или 161 миллиард ГБ), что в ряде стран принимаются специальные «цифровые» законодательные акты. Однако далеко не все компании сегодня действительно задумываются над вопросом «Что такое ИБ и какие практические меры должны быть запланированы и внедрены в каждой конкретной организации для обеспечения режима ИБ?». Авторы в данной статье предоставляют методическую базу для самостоятельного ответа на этот вопрос.

Теория, необходимая практикам

Специалисты по ИБ выделяют 3 специфические области для анализа и оценки защищенности: обеспечение целостности, доступности и конфиденциальности информации. Применяют математически выверенные формулировки, которые позволяют предельно точно описать сложные взаимоотношения объектов, субъектов, политик доступа и иных «узких» специфических терминов. В общих чертах определить эти области можно так:

- ✓ целостность – это способность обеспечить неизменность исходной информации. Любые изменения информации по сравнению с ее исходным видом (например, «лишний» нолик в платежке или «новая» дата платежа в контракте) должны быть обнаружены точно.
- ✓ доступность – это способность обеспечить доступ к определенной информации для легальных пользователей в определенный временной интервал (например, работа портала приема платежей банка 24x7x365);
- ✓ конфиденциальность – это способность обеспечить защиту (тайну) передаваемой информации от посторонних. Это качество особенно актуально при возможном активном вмешательстве недоброжелателей (конкурентов или хакеров).

Примечание:

Стандарт ISO/IEC 13335-1:2004 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» устанавливает следующие формальные основные термины:

✓ **Доступность (availability):** Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

- ✓ **Конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.
- ✓ **Целостность** (integrity): Свойство сохранения правильности и полноты активов.

Какие способы защиты данных и средства защиты информации использовать – каждая организация решает, исходя из своих оценок допустимого риска и сопоставимых финансовых возможностей. Наиболее широко используются различные средства шифрования (криптографической защиты как информации, так и каналов связи), решения по контролю доступа (аутентификация, авторизация, биометрические системы) и различные инструментальные средства, решающие узкие специализированные задачи (системы анализа вторжений, сканеры безопасности, межсетевые экраны и иные).

Менеджмент рисков представляет собой центральное и важнейшее требование при обеспечении ИБ, т.к. позволяет построить систему оценок, удобных для принятия решения высшим менеджментом организации. Как правило, специалисты применяют две основные методики – качественной и количественной оценки.

Пример качественной модели оценки рисков

Последствия	Незначительные	Значительные	Катастрофические
Вероятность			
Очень вероятно	Высокий риск	Недопустимый риск	Недопустимый риск
Вероятно	Средний риск	Высокий риск	Недопустимый риск
Маловероятно	Низкий риск	Средний риск	Высокий риск
Почти невероятно	Низкий риск	Низкий риск	Средний риск

Пример количественной модели оценки рисков

Вероятность	0,9				Зона приемлемого риска
	0,8				
	0,7				
	0,6				
	0,5		Зона допустимого риска		
	0,4				
	0,3	Зона минимального риска			
	0,2				
	0,1				
		10	100	1.000	5.000
Сумма причиненных убытков (USD x 1.000)					

Сегодня для каждой области ИБ предлагаются несколько (иногда свыше сотни) решений в широком ценовом и функциональном диапазоне. Каждая организация может провести исследование текущего состояния своей системы защиты (аудит ИБ) и подготовить модель рисков (какие внешние события наиболее критичны для бизнеса в случае наступления). По итогам исследования текущего состояния своей системы защиты (аудита ИБ) возможен выбор конкретных технологий (решений) по минимизации ущерба (последствий рисков) в соответствии с принятой политикой ИБ.

Примечание:

Стандарт ISO/IEC 27001:2005 устанавливает понятие ИБ:

✓ **информационная безопасность** (information security): Сохранение конфиденциальности, целостности и доступности информации; кроме того, могут охватываться и другие свойства, такие как аутентичность (достоверность), возможность идентификации, неотказуемость и надежность [ИСО/МЭК 17799:2005]

Важно обратить внимание, что понятие «ИБ» не ограничивается только средствами (решениями). Необходимо обеспечить именно систему ИБ как совокупность средств («железа» и / или программного обеспечения) и персонала, ответственного за функционирование технических средств защиты. Невозможно обеспечить эффективный режим ИБ без комплекса требований: к персоналу, к использованию мобильных накопителей («флешек»); без внедрения организационных мер и системы внутренних проверок (аудитов).

Соответствие законодательству

Каждая организация вправе вести бизнес так, как это необходимо в данной стадии ее развития при неукоснительном соблюдении норм законодательства – правило, общее для всех, ведущих цивилизованный бизнес. Законы хорошо известны и бухгалтерам и юристам, но их знание не менее важно и для создания эффективной системы менеджмента ИБ (СМИБ).

По данным PWC (2009) соблюдение законодательства – критичный фактор обеспечения ИБ, и, прежде всего, для организации как владельца ценных активов.

Рисунок 2. Причины, увеличивающие мотивацию и давление внешних обстоятельств для совершения мошеннических действий*



Примечание:

Стандарт ISO/IEC 27001:2005 устанавливает понятие СМИБ:

система менеджмента защиты информации СМИБ

[information security management system] [ISMS] - часть общей системы менеджмента, основанной на подходе деловых рисков, с целью создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать защиту информации,

ПРИМЕЧАНИЕ: Система менеджмента включает организационную структуру, политику, деятельность по планированию, ответственность, практики, процедуры, процессы и ресурсы.

Любая организация должна защищать свои информационные активы - например, определяя необходимым условием для их использования режим коммерческой тайны. В этом режиме любой пользователь информационной системы организации подписывает обязательство о неразглашении конфиденциальной информации (который включает список категоризированной информации, например: стратегические маркетинговые программы, торговые объемы, структура информационных ресурсов) и информируется об ответственности за нарушение режима ИБ.

Примечание:

Стандарт ISO/IEC 27001:2005 устанавливает требования к СМИБ:

А.15.1 Соответствие требованиям законодательства.

Цель: Избегать любых нарушений действующего законодательства или договорных обязательств, а также любых требований безопасности.

А.15.2 Соответствие политикам и стандартам безопасности, а также техническое соответствие.

Цель: Гарантировать соответствие систем организационным политикам и стандартам безопасности.

Для экспертов в области ИБ очень важно четко установить, а в ряде случаев выполнить сегментацию «маршрутов» информационного обмена в информационной системе своей организации с целью определения применимых правил и требований по внедрению СМИБ.

Каждая организация самостоятельно может определять, помимо режима ИБ, средства или комбинации средств ИБ, применяемые, например, при построении внутреннего документооборота или безопасной корпоративной почты. Важное замечание: при взаимодействии информационных систем организации и государственных органов (например, налоговые инспекции) необходимо использовать рекомендованные средства защиты. Также настоятельно рекомендуется применять требования ИСО 27001 к СМИБ в части касающейся проведения проверок (аудитов) информационных активов (систем) в организации.

Примечание:

Стандарт ISO/IEC 27001:2005 устанавливает требования к СМИБ:

А.15.3 Вопросы аудита информационных систем

Цель: Максимизация результативности процесса аудита информационных систем и минимизация негативного влияния, связанного с данным процессом.

Средства защиты информации

Принимая во внимание широчайший перечень всех возможных схем построения корпоративных информационных систем (КИС) предлагается сосредоточить внимание на трех ключевых «рубежах защиты»: сервера, рабочие станции и сетевая инфраструктура. Целесообразно принять во внимание, что в последнее время достаточно известная и практически отработанная схема «периметра защиты», при которой вся сеть организации защищалась единственным межсетевым экраном в единственной точке выхода в Интернет, существенно устарела.

Прежде всего, изменилась концепция работы современного офиса: беспроводные (Wi-Fi, WiMAX) устройства позволяют работать в любой точке мира, где есть покрытие сети сотовой связи (практически в каждом аэропорту сотни человек работают на своих ноутбуках через беспроводные точки доступа). Необходимо защищать не только и не столько один «вход» в сеть, а каждое устройство, которое и стало сетью. Далее: многочисленные мобильные устройства (коммуникаторы), способные подключаться к рабочим компьютерам, оснащенные слотами SD/MMC, USB и поддерживающие несколько беспроводных протоколов. В таком сложном хитросплетении устройств, протоколов и серверов для создания эффективной системы ИБ будет полезно сосредоточиться на предложенных областях:

- ✓ Решения для рабочих станций: обеспечить защиту от постороннего доступа (пароли, строгие политики авторизации, шифрование персональных данных, антивирусы). Для ноутбуков топ-менеджеров, где содержится наиболее ценная информация, рекомендуется шифрование дисков, запрет подключения через USB-порты, отключение беспроводных протоколов. В случае несанкционированного доступа или хищения такого ноутбука доступ к ценной коммерческой информации будет невозможен или существенно затруднен;
- ✓ Решения для серверов: защита от постороннего доступа (аппаратная защита с помощью «электронных замков»), защита от внешнего вторжения (помещение в «демилитаризованную зону», шифрование данных, строгие политики доступа, системы анализа вторжений и анализаторы трафика;
- ✓ Решения для сетей - применение современных межсетевых экранов (МЭ), интегрированных с системами анализа контента, анализаторов спама и поддержкой «туннелей» (VPN), применение технологий цифровых сертификатов (PKI);

На практике СЗИ применяются с учетом ряда факторов: цена, сравнительный уровень предоставляемых функций, простота установки и управления, возможность интеграции в единую систему управления ИБ. Важно отметить, что образ «крутого» ситуационного центра, где за десятком мониторов напряженно работает команда «безопасников», остался только на экранах боевиков. Все компоненты современной системы ИБ управляются с единой консоли, одновременно ведется автоматизированное управление несколькими событиями от множества сенсоров. Это достигается интеграционными решениями: все известные «узкие» игроки рынка ИБ в мире уже поглощены крупнейшими лидерами рынка ПО (например, IBM приобрела крупнейшего игрока рынка ИБ – компанию ISS). Клиентам предоставляются уже собранные и протестированные решения: функциональные «базовые» (например, учетные системы, сетевое оборудование) и компоненты ИБ – конечному пользователю не нужно больше настраивать «ручками».

Например, компания Cisco предлагает ряд «узких» решений ИБ, интегрируемых в коммутаторы и маршрутизаторы локальных сетей:

- ✓ по обнаружению и предотвращению атак (IDSM-2),
- ✓ для фильтрации Web-трафика и аутентификации (Cisco Content Engine Network Module),
- ✓ решение для обнаружения атак (Cisco IDS Network Module),

С экономической точки зрения СМИБ строится не на закупке «железа», а, прежде всего, на продуманной политике применения комплекса мер (в т.ч. административных), способных снизить риски ИБ до приемлемого «остаточного» уровня. Очевидно, что совокупная стоимость всей СМИБ должна учитывать критичность допустимых для данного бизнеса потерь – например, известна ситуация, возникшая в результате сбоя в технической системе ММВБ (Московской Международной Валютной Биржи) 12.04.2007 г., когда американский доллар в течение целых 28 минут стоил 14 рублей.

Создание модели нарушителя

Очевидно, что вся современная, отлично настроенная и постоянно обновляемая система ИБ будет просто «мертвым железом» без тщательной и выверенной работы с персоналом. Вопрос мотивации персонала любой компании особо актуален сегодня, когда на рынке труда высокий спрос на специалистов самого разного профиля. Попробуем определить, какие риски могут нести нелояльные сотрудники для организации с позиции ИБ.

Прежде всего, нелояльный пользователь может успешно игнорировать правила и политики в этой области (ибо ни одна система защиты не может запретить все для каждого пользователя – тогда она не нужна). Возможен несанкционированный вынос конфиденциальной информации на USB-флешках, «лишняя» распечатка, «забытая» резервная копия диска и пр. Часто на столах и компьютерах забывчивых и неаккуратных пользователей можно наблюдать приклеенные листочки с паролями, открытые шкафы с документами, стопки неразобранных распечаток у сетевого принтера и пр. На столах у «очень занятых начальников» часто можно видеть распечатки Excel с финансовыми планами подразделений, списками на премирование сотрудников, графики поступления платежей от клиентов и пр. – и таких примеров множество, к сожалению...

К чему может привести такая неаккуратность и забывчивость? По данным экспертов «Русского Регистра» во многих случаях утечка критических данных могла бы быть предотвращена, если бы руководство компаний выполняло бы минимальные требования ИБ.

Примечание:

Стандарт ISO/IEC 27001:2005 содержит требования к СМИБ:

- ✓ **А.8.3.3 Удаление прав доступа** – Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации должны быть удалены по истечении срока их найма, действия договора или соглашения, или скорректированы после изменения.
- ✓ **А.9.2.7 Вынос имущества** – Оборудование, информация или ПО не могут быть вынесены из помещения организации без соответствующего разрешения.
- ✓ **А.10.7.2 Утилизация носителей информации** – Носители информации, когда в них больше нет необходимости, должны надежно и безопасно утилизироваться, используя формальные процедуры.

Ваши конкуренты будут очень рады получить самые свежие данные со стола менеджеров компании – и документы не нужно даже похищать с применением суперсовременных шпионских технологий: просто положить на ксерокс и вернуть оригинал на место. Известны случаи хищения ноутбуков в транспорте (в метро в часы пик) или из автомобилей. Конечно, стоимость информации в несколько раз превышает стоимость просто ноутбука, даже нового; снять информацию с жесткого диска не составляет особого труда.

Стандарты ИБ

Определяем базис для формирования требований к СМИБ, это, прежде всего, семейство стандартов серии 27000:

- ✓ ISO/IEC 27000:2009 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Общие положения и словарь».
- ✓ ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».
- ✓ ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».
- ✓ ISO/IEC 27005:2008 «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности».
- ✓ ISO/IEC 27006:2007 «Информационные технологии. Средства обеспечения безопасности. Требования для органов, выполняющих аудит и сертификацию систем менеджмента информационной безопасности».
- ✓ ISO/IEC 27011:2008 «Информационные технологии. Средства обеспечения безопасности. Руководящие указания по менеджменту информационной безопасности для телекоммуникаций».
- ✓ ISO/IEC 27799:2008 «Информатизация здравоохранения. Менеджмент информационной безопасности для здравоохранения».

Базовый (сертифицирующий) стандарт ISO/IEC 27001:2005

Стандарт ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования» устанавливает требования к СМИБ для любой организации, вне зависимости от ее размеров, отраслевой принадлежности и географического места расположения. Стандарт предназначен для обеспечения адекватного выбора эффективных средств ИБ, в строгом соответствии с принятой в организации политикой информационной безопасности, практикой менеджмента рисков и другими необходимыми процедурами. Внедрение СМИБ в соответствии с требованиями стандарта выполняется в несколько этапов, при этом важно обеспечить вовлечение в процесс всего персонала организации, имеющего дело с ценными активами.

Обеспечение информационной безопасности и кризис?

Для развития технологий ИБ и создания СМИБ в частности, важно оценить не только технические и законодательные требования, но и выполнить экономические расчеты. В текущей экономической ситуации вопросы эффективности (т.е. соотношения достигнутого результата и затраченных ресурсов) получили приоритет. На портале SecurityLab (данные обзора 30.12.2008 г.) опубликованы результаты опросов по проблеме важности ИБ. «...Как оказалось, даже в столь неблагоприятном климате на рынке важность ИБ не вызывает сомнений...»

- ✓ **50,6 % участников исследования считают, что защита корпоративных секретов всегда является первоочередной задачей,**
- ✓ **22,7 % респондентов заявили, что укрепление ИБ особенно важно в кризисные времена для повышения конкурентоспособности.**
- ✓ **5,2 % специалистов считают, что сэкономить можно и на безопасности.**

Основные направления внедрения СМИБ

Эксперты «Ассоциации по сертификации «Русский Регистр» предлагают следующие основные направления внедрения СМИБ, исходя из известных современных технических и технологических требований:

Внедрение международных практик безопасности

Применение в организациях лучших практик, основанных на международных стандартах, позволит создать современную и экономически эффективную систему ИБ для всех участников делового сотрудничества.

Пример: ISO/IEC 27001:2005, ITIL, CobIT,...

Внедрение системы менеджмента рисков

Наличие методологии менеджмента рисков СМИБ позволит обеспечить управляемые условия для снижения ущерба от возможных негативных воздействий на активы организаций, прежде всего, направленных на персонал и конфиденциальную информацию.

Пример: ISO/IEC 27005:2005, ISO 14971, ISO 18044, CobIT Security, Basel-II,...

Внедрение конкретных средств защиты

Задача обеспечения национальной безопасности требует проектирования и внедрения комплексной систем безопасности в организациях. В процессе создания СМИБ реализуется внедрение комплекса технических и иных средств защиты, в соответствии с адекватной моделью угроз и уязвимостей.

Пример: «Типовая модель нарушителя»

Разработка типовой модели обеспечения комплексной безопасности:

Эксперты «Ассоциации по сертификации «Русский Регистр» предлагают к применению типовую модель комплексной безопасности, основанной на требованиях международного стандарта ISO/IEC 27001:2005. Кратко рассмотрим основные элементы типовой модели:

- ✓ Идентификация активов;
- ✓ Идентификация угроз и уязвимостей к конкретным активам;
- ✓ Оценка рисков, в т.ч. разработка плана непрерывности бизнеса;

- ✓ Разработка типовых политик безопасности;
- ✓ Рекомендация выбора конкретных средств защиты активов;
- ✓ Рекомендация по сертификации систем менеджмента предприятий;
- ✓ Практическое изучение (стажировка) на типовой модели безопасности.

Схемы внедрения и сертификации

Эксперты «Ассоциации по сертификации «Русский Регистр» предлагают следующие две типовые схемы внедрения с последующей сертификацией СМИБ в соответствии с требованиями международного стандарта ISO/IEC 27001:2005:

1. Разработка, внедрение и сертификация СМИБ:

Внедряется СМИБ как самостоятельная (первая) система менеджмента в Организации. Вопрос интеграции не ставится в момент принятия решения о создании СМИБ.

2. Внедрение СМИБ в составе интегрированных систем менеджмента:

- ISO 9001:2008
- ISO 14001:2004
- ISO 18001:2007

Внедряется СМИБ в составе единой системы менеджмента в Организации.

Вопрос интеграции изначально изучается в процессе принятия решения о создании (интеграции) СМИБ.