Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 7 (158)/2006

Подходы компании «Инфосистемы Джет» к информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Подходы компании «Инфосистемы Джет» к информационной безопасности

СОДЕРЖАНИЕ

Введение

Обеспечение информационной безопасности (ИБ) является сегодня одним из основных требований к информационным технологиям (ИТ). Причина этого — неразрывная связь ИТ и основных бизнес-процессов в любых организациях, будь то государственные службы, промышленные предприятия, финансовые структуры, операторы телекоммуникаций. Вместе с тем в практической работе по обеспечению информационной безопасности существует ряд проблем, связанных со старыми подходами к созданию и развитию информационных систем (ИС). В числе таких проблем можно указать следующие:

- Неправильная оценка перспектив развития системы, в результате чего у системы не остается возможностей для количественного либо качественного роста, из-за чего требуется существенная перестройка системы практически сразу же после ее построения. С точки зрения информационной безопасности набор средств защиты и процедур, регулирующих защиту информации, значительно снижает показатели системы и создает условия для отказа от использования средств защиты в процессе эксплуатации.
- Привязка к жестко определенной инфраструктуре обуславливается обычно стремлением использовать известные и, как правило, давно применяющиеся технологии. Как следствие, при необходимости перехода на другие технологии систему невозможно динамично модернизировать в обозримые сроки и без значительных затрат.
- Невозможность разделения инфраструктурной и прикладной компонент является естественным следствием ситуации, когда система строится в расчете на определенные инфраструктурные решения. В результате создается защищенная инфраструктура, но информация, обрабатываемая в прикладных системах, остается незащищенной.
- Маркетинговый подход к выбору технологий и продуктов не позволяет объективно оценить свойства технологий и решений, предлагаемых различными поставщиками. При этом поставщики указывают на преимущества решений и умалчивают о недостатках. Недостатки же могут сделать систему существенно менее привлекательной, а в ряде случаев — и вовсе не отвечающей предъявляемым к ней требованиям.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность предприятия обеспечивается в случае сохранения следующих свойств информационной системы:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Основными задачами обеспечения информационной безопасности являются:

- создание механизмов своевременного выявления, прогнозирования, локализации и оперативного реагирования на угрозы безопасности и проявления негативных тенденций в использовании информационных ресурсов и систем;
- создание эффективной нормативно-правовой базы обеспечения информационной безопасности;
- создание технологической и материально-технической базы информационной безопасности;
- обеспечение правовой защиты субъектов информационных отношений;
- сохранение и эффективное использование информационных ресурсов;
- координация деятельности органов государственной власти, организаций и предприятий отрасли в обеспечении информационной безопасности;
- унификация требований к обеспечению информационной безопасности;
- создание комплексной системы информационной безопасности и контроля эффективности принимаемых мер защиты;
- обеспечение надежного функционирования информационных систем и предоставляемых ими услуг.

Работы по защите информации должны проводиться поэтапно с участием руководства и персонала подразделений, осуществляющих хранение и обработку информации. Этапы работ включают:

- категорирование информации;
- анализ структуры информационных ресурсов и значимых рисков;
- планирование и реализация организационных мер;
- проектирование и внедрение программно-технических средств защиты информации.

Важным с точки зрения эффективности применяемых решений является их соответствие заданным требованиям, которые, в свою очередь, обосновываются анализом рисков, проведенным для конкретной системы в соответствии с международно признанными методиками.

Опыт показывает, что определяющими для успешной реализации системы информационной безопасности в организации являются следующие факторы:

- цели безопасности и ее обеспечение основываются на производственных целях и требованиях, функции управления безопасностью выполняет руководство организации;
- явная поддержка и приверженность высшего руководства к поддержанию режима безопасности;
- адекватное понимание рисков нарушения безопасности (как угроз, так и слабостей), которым подвергаются ресурсы организации, и уровня их защищенности, который основывается на ценности и важности этих ресурсов;
- ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации;
- предоставление исчерпывающего пособия по политике и стандартам информационной безопасности всем сотрудникам и подрядчикам.

Эффективная эксплуатация большой высококритичной системы требует не только расширенного технического обслуживания, но и ряда услуг консалтингового характера. Эффективность использования всех предлагаемых услуг в первую очередь зависит от того, насколько точно описаны текущие требования к эксплуатации и планы развития всей ИТ-инфраструктуры организации.

Попытки решить проблемы безопасности внедрением того или иного средства являются неэффективной тратой денег, поскольку не обеспечивают полноты необходимого набора мер защиты. Только комплексный, систематический подход позволит успешно противостоять нарастающим угрозам. Различные аспекты такого подхода к решению современных проблем информационной безопасности раскрываются в представленных здесь материалах.

Создание комплексной системы управления информационной безопасностью

Василий Носаков,
руководитель группы аудита и консалтинга

В конце 2005 года в свет вышел новый международный стандарт в области информационной безопасности — BS ISO/IEC 27001:2005 (далее Стандарт). В данном документе сформулированы требования к системе управления информационной безопасностью (СУИБ), включая общую методологию создания, внедрения и оценки эффективности механизмов СУИБ.

В настоящее время наблюдается повышенный интерес к этому стандарту со стороны компаний, работающих в различных отраслях. Соответствие ему становится важным фактором коммерческого успеха организации благодаря целому ряду преимуществ, которые она получает, таким как:

- конкурентные преимущества;
- повышение положения компании в международных рейтингах, необходимое для привлечения зарубежных инвестиций и выхода на международные рынки;
- повышение стоимости акций компании;
- демонстрация партнерам и клиентам высокого уровня своей надежности за счет адекватной защиты информации, включая информацию клиентов и партнеров;
- снижение рисков, связанных с возможными ущербами для активов компании;
- повышение прозрачности процесса управления информационной безопасностью в организации:
  - четкое разделение полномочий и ответственности за обеспечение информационной безопасности;
  - критерии оценки эффективности выполняемых мероприятий по обеспечению информационной безопасности;
  - обоснование затрат на информационную безопасность.

Перечисленные здесь преимущества приобретаются в результате получения сертификата соответствия СУИБ организации требованиям BS ISO/IEC 27001:2005, который выдается независимым органом по сертификации при успешном прохождении сертификационного аудита СУИБ.

Самым трудоемким и сложным этапом на пути к сертификации является собственно создание системы управления ИБ и внедрение ее механизмов в компании.

В данной статье рассмотрены основные компоненты и этапы создания СУИБ, соответствующей требованиям BS ISO/IEC 27001:2005.

ISO/IEC 27001 и система управления информационной безопасностью

Стандарт BS ISO/IEC 27001:2005 представляет собой модель системы менеджмента в области информационной безопасности. Как и любая другая современная система менеджмента, СУИБ — это, прежде всего, набор организационных мероприя-

Рис.1. Процессный подход в рамках СУИБ

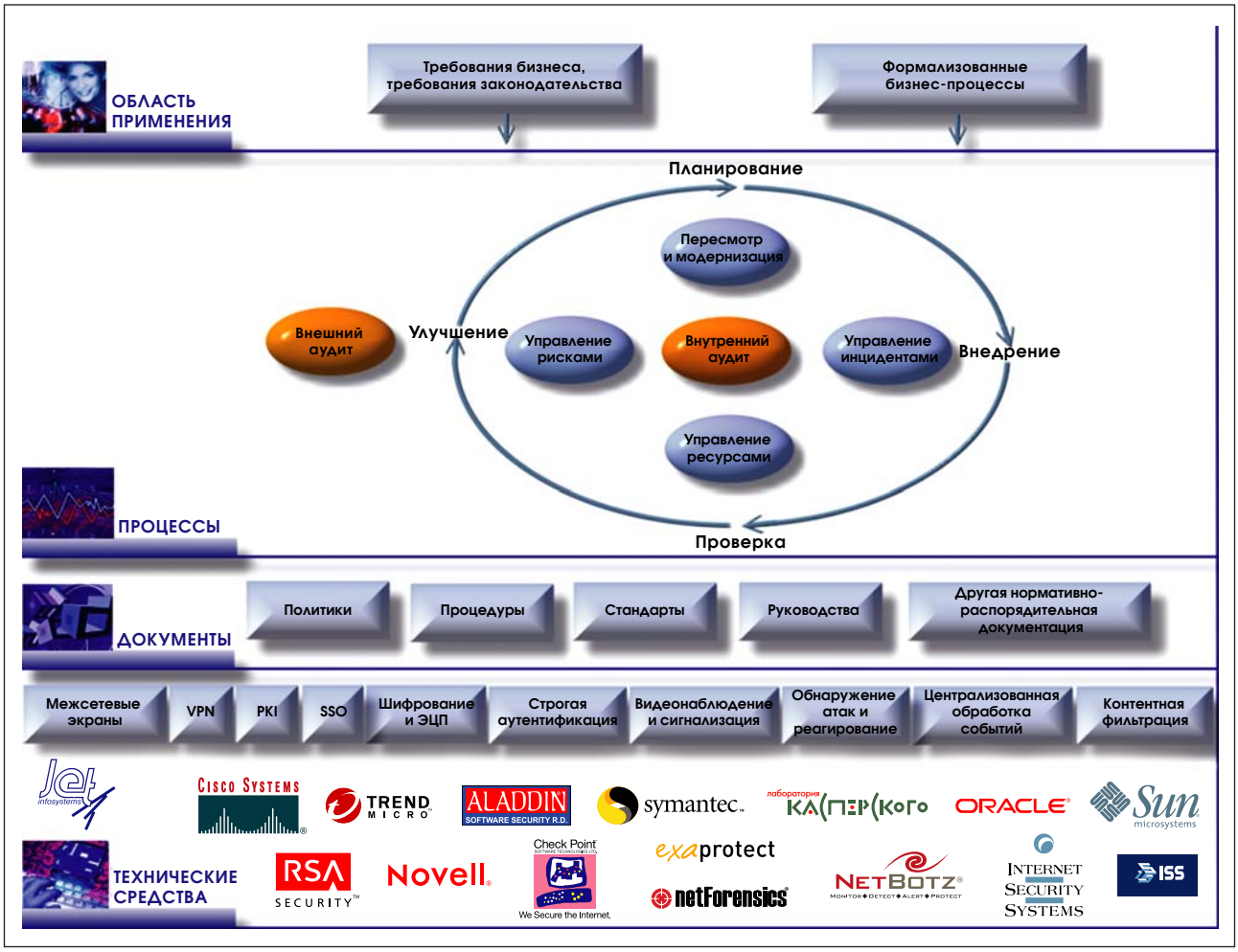

Рис.2. Комплексная система управления информационной безопасностью

Рис.3. Место СУИБ в общей системе менеджмента организации

тий и процедур управления, она не является по своей сути техническим стандартом.

В основе стандарта лежит процессный подход к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ компании. Он заключается в создании и применении системы процессов управления, которые взаимоувязаны в непрерывный цикл планирования, внедрения, проверки и улучшения СУИБ (Рис.1).

Дополнительно в Стандарте приведен перечень механизмов защиты информации программно-технического уровня, который может использоваться. Таким образом, СУИБ, построенная в соответствии с требованиями ISO/IEC 27001:2005, представляет собой комплексную систему, включающую и механизмы управления, и механизмы защиты информации (Рис.2).

Основным движущим механизмом СУИБ является периодический анализ рисков информационной безопасности. Высшее руководство организации также вовлекается в процесс управления СУИБ посредством принятия решений на основе результатов анализа рисков, результатов внутренних аудитов и других механизмов СУИБ. С точки зрения процессов управления СУИБ входит в общую систему менеджмента организации и предоставляет дополнительные механизмы управления в части обеспечения защиты критичной информации (Рис.3).

Этапы создания СУИБ

В рамках работ по созданию СУИБ можно выделить следующие основные этапы:

1. Принятие решения о создании СУИБ.
2. Подготовка к созданию СУИБ.
3. Анализ рисков.
4. Разработка политик и процедур СУИБ.
5. Внедрение СУИБ в эксплуатацию.

Рассмотрим данные этапы более подробно.

Принятие решения о создании СУИБ

Решение о создании и последующей сертификации СУИБ должно приниматься высшим руковод-

ством организации. Таким образом руководство выражает свою поддержку началу данного процесса, что является ключевым фактором для успешного внедрения СУИБ в организации. При этом руководство должно осознавать конечную цель данного мероприятия и ценность сертификации для бизнеса компании.

Подготовка к созданию СУИБ

Организация рабочей группы

Не менее важным фактором успешного внедрения СУИБ является создание рабочей группы, ответственной за внедрение СУИБ. В ее состав должны войти:

- представители высшего руководства организации;
- представители бизнес-подразделений, охватываемых СУИБ;
- специалисты подразделений, обеспечивающих информационную безопасность в компании, имеющие соответствующее образование или подготовку, знающие основные принципы и лучшие практики в области информационной безопасности.

Перечисленные сотрудники должны понимать универсальные механизмы систем менеджмента, знать требования Стандарта и пройти обучение по вопросам создания и эксплуатации СУИБ.

В состав рабочей группы, кроме сотрудников компании, могут входить также привлеченные консультанты, специализирующиеся в вопросах построения СУИБ.

Хорошей практикой является создание в организации комитета по информационной безопасности, который, кроме вопросов, связанных с внедрением СУИБ, должен на постоянной основе обеспечить решение задач, определяемых эксплуатацией данной СУИБ и ее непрерывным совершенствованием.

Нормативно-методическое обеспечение

Рабочая группа должна иметь в своем распоряжении всю необходимую нормативно-методическую базу для успешного создания системы управления информационной безопасностью, соответствующей требованиям Стандарта. К сожалению, в настоящий момент изданы далеко не все необходимые документы, что безусловно затрудняет внедрение требований Стандарта.

Ниже приведены стандарты и методики, которыми следует руководствоваться:

- ISO/IEC 27000 — Словарь и определения. Дата выхода неизвестна.
- ISO/IEC 27001:2005.
- ISO/IEC 27002. Сейчас: ISO/IEC 17799:2005. Дата выхода — 2007 год.
- ISO/IEC 27003. Руководство по внедрению СМИБ. Дата выхода — 2008 год.
- ISO/IEC 27004. Метрики ИБ. Дата выхода неизвестна.
- ISO/IEC 27005. Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
- ISO/IEC 27006. «Guidelines for information and communications technology disaster recovery services». Сейчас: SS507:2004 — Singapore Standards for Business Continuity/Disaster Recovery (BC/DR) Service Providers. Дата выхода неизвестна.
- ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards.
- ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security managment.
- ISO/IEC TR 18044 Information technology — Security techniques — Information security incident management.
- ISO/IEC 19011:2002 Guidelines for quality and / or environmental management systems auditing.
- Серия методик Британского института стандартов по созданию СУИБ (ранее: документы серии PD 3000).

Выбор области деятельности организации, которая будет охвачена СУИБ

При выборе области деятельности, в которой силами специально созданной рабочей группы будут внедряться механизмы СУИБ, должны учитываться следующие факторы:

- деятельность и услуги, предоставляемые организацией своим партнерам и клиентам;
- целевая информация, безопасность которой должна быть обеспечена;
- бизнес-процессы, обеспечивающие обработку целевой информации;
- подразделения и сотрудники организации, задействованные в данных бизнес-процессах;
- программно-технические средства, обеспечивающие функционирование данных бизнес-процессов;
- территориальные площадки компании, в рамках которых происходят сбор, обработка и передача целевой информации.

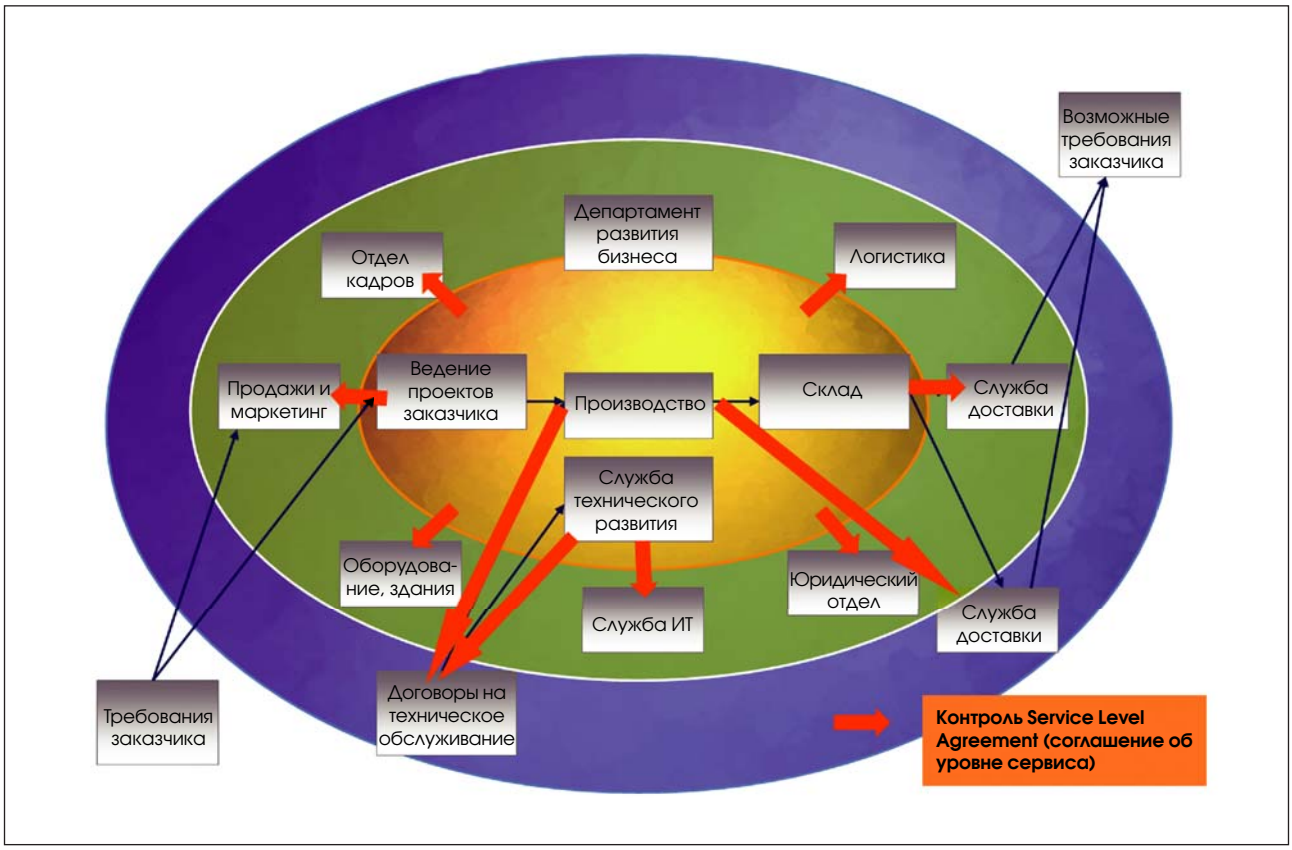

Рис.4. Пример области деятельности

Результатом является согласованная с высшим руководством область деятельности организации, в рамках которой планируется создание СУИБ (Рис. 4).

Выявление несоответствий

Для уточнения объема работ и необходимых затрат на создание и последующую сертификацию СУИБ члены рабочей группы проводят работы по выявлению и анализу несоответствий существующих в организации мер защиты требованиям Стандарта. При этом анализируются как применяемые организационные мероприятия в области планирования, внедрения, аудита и модернизации мер по обеспечению информационной безопасности, так и используемые программно-технические средства и механизмы защиты информации.

На данном этапе компания также может выбрать независимый орган по сертификации систем менеджмента, имеющий соответствующую аккредитацию, в котором она хотела бы пройти сертификацию.

Хорошей практикой является заказ у органа по сертификации предварительного аудита для выявления существующих на текущий момент несоответствий требованиям Стандарта. Предварительный аудит на данном этапе поможет выявить области, требующие усовершенствования.

Результатом этих работ должен стать перечень несоответствий требованиям Стандарта и план работ по созданию СУИБ организации.

Анализ рисков

Одной из наиболее ответственных и сложных задач, решаемых в процессе создания СУИБ, следует назвать проведение анализа рисков информационной безопасности в отношении активов организации в выбранной области деятельности и принятие высшим руководством решения о выборе мер противодействия выявленным рискам.

В процессе анализа рисков проводятся следующие работы:

- идентификация всех активов в рамках выбранной области деятельности;
- определение ценности идентифицированных активов;
- идентификация угроз и уязвимостей для идентифицированных активов;
- оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;

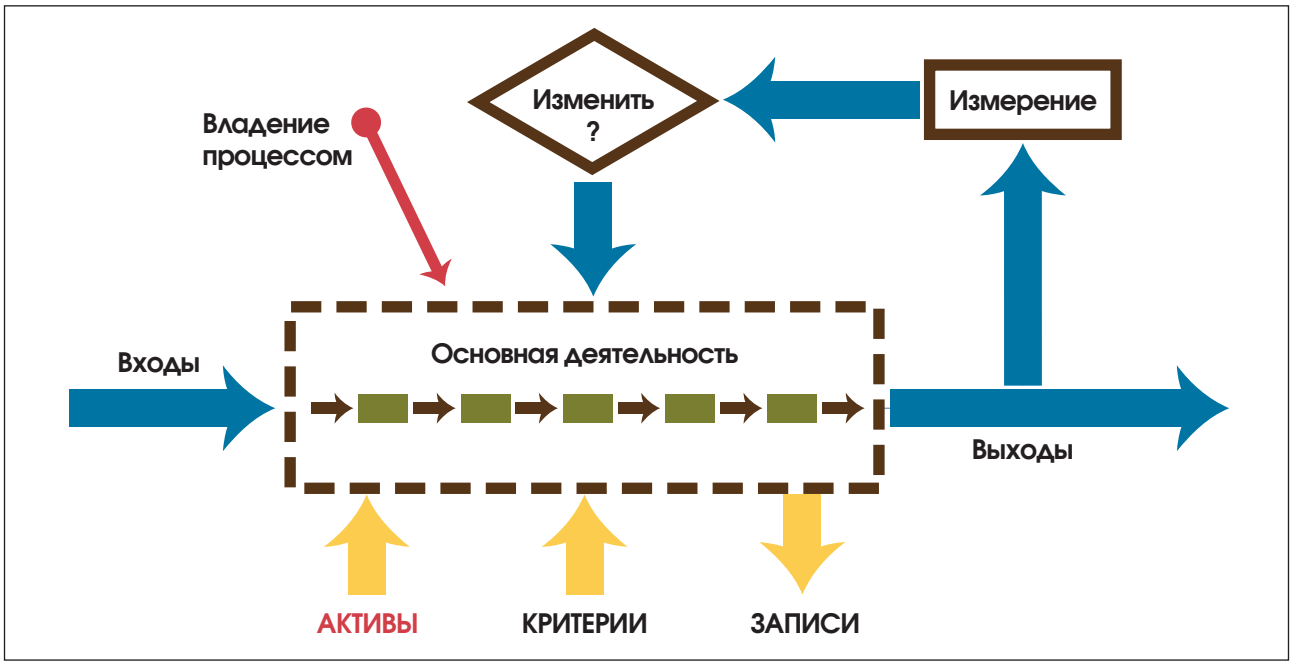

Рис.5. Идентификация активов в бизнес-процессах

- выбор критериев принятия рисков;
- подготовка плана обработки рисков.

Выполнение всех указанных задач обычно осуществляется в соответствии с разрабатываемой процедурой анализа рисков, в которой определена методология и отражены организационные аспекты по каждой из задач.

Идентификация и определение ценности активов

В рамках данных работ должны быть рассмотрены все бизнес-процессы, входящие в выбранную область деятельности организации. По каждому бизнес-процессу совместно с владельцем процесса производится идентификация задействованных активов (Рис. 5).

В терминах Стандарта под активами понимаются:

- информационные входные данные;
- информационные выходные данные;
- информационные записи;
- ресурсы: люди, инфраструктура, оборудование, программное обеспечение, инструменты, услуги.

Следующим шагом в проведении анализа рисков ИБ в отношении активов компании является определение ценности актива, которая выражается в величине ущерба для организации, если нарушается какое-либо из следующих свойств актива: конфиденциальность, целостность, доступность.

Информация о ценности актива может быть получена от его владельца или же от лица, которому владелец делегировал все полномочия по данному активу, включая обеспечение его безопасности.

Результатом данных работ является отчет об идентификации и оценке ценности активов.

Анализ рисков

Анализ рисков – это основной движущий процесс СУИБ. Он выполняется не только при создании СУИБ, но и периодически при изменении бизнес-процессов организации и требований по безопасности.

Необходимо подобрать такую методику анализа рисков, которую можно было бы использовать с минимальными изменениями на постоянной основе. Есть два пути: использовать существующие на рынке методики и инструментарий для оценки рисков или же разработать свою собственную методику, которая наилучшим образом будет подходить к специфике компании и охватываемой системой управления информационной безопасности области деятельности.

Последний вариант наиболее предпочтителен, поскольку пока большинство существующих на рынке продуктов, реализующих ту или иную методику анализа рисков, не отвечают требованиям Стандарта. Типичными недостатками таких методик являются:

- стандартный набор угроз и уязвимостей, который зачастую невозможно изменить;

- принятие в качестве активов только программно-технических и информационных ресурсов — без рассмотрения человеческих ресурсов, сервисов и других важных ресурсов;
- общая сложность методики с точки зрения ее устойчивого и повторяющегося использования.

В процессе анализа рисков для каждого из активов или группы активов производится идентификация возможных угроз и уязвимостей, оценивается вероятность реализации каждой из угроз и, с учетом величины возможного ущерба для актива, определяется величина риска, отражающего критичность той или иной угрозы.

Необходимо отметить, что в соответствии с требованиями Стандарта в процедуре анализа рисков должны быть идентифицированы критерии принятия рисков и приемлемые уровни риска. Эти критерии должны базироваться на достижении стратегических, организационных и управленческих целей организации.

Высшее руководство компании использует данные критерии, принимая решения относительно принятия контрмер для противодействия выявленным рискам. Если выявленный риск не превышает установленного уровня, он является приемлемым, и дальнейшие мероприятия по его обработке не проводятся. В случае же, когда выявленный риск превышает приемлемый уровень критичности угрозы, высшее руководство должно принять одно из следующих возможных решений:

- снижение риска до приемлемого уровня посредством применения соответствующих контрмер;
- принятие риска;
- избежание риска;
- перевод риска в другую область, например, посредством его страхования.

Реализация плана обработки рисков

В соответствии с принятыми решениями формируется план обработки рисков. Данный документ содержит перечень первоочередных мероприятий по снижению уровней рисков, а также цели и средства управления из «Приложения А» Стандарта, направленные на снижение рисков, с указанием:

- лиц, ответственных за реализацию данных мероприятий и средств;
- сроков реализации мероприятий и приоритетов их выполнения;
- ресурсов для реализации таких мероприятий;
- уровней остаточных рисков после внедрения мероприятий и средств управления.

Принятие плана обработки рисков и контроль за его выполнением осуществляет высшее руководство организации. Выполнение ключевых мероприятий плана является критерием, позволяющим принять решение о вводе СУИБ в эксплуатацию.

Разработка политик и процедур СУИБ

Разработка организационно-нормативной базы, необходимой для функционирования СУИБ, может проводиться параллельно с реализацией мероприятий плана обработки рисков.

На данном этапе разрабатываются документы, явно указанные в Стандарте, а также те, необходимость реализации которых вытекает из результатов анализа рисков и из собственных требований компании к защите информации. Обычно сюда входят следующие основные политики и процедуры:

- область деятельности СУИБ;
- политика СУИБ;
- подполитики по основным механизмам обеспечения информационной безопасности, применимым к выбранной области деятельности, охватываемой СУИБ, такие как:
  - политика антивирусной защиты;
  - политика предоставления доступа к информационным ресурсам;
  - политика использования средств криптографической защиты;
  - другие политики;
- процедуры СУИБ:
  - управление документацией;
  - управления записями;
  - внутренние аудиты;
  - корректирующие действия;
  - предупреждающие действия;
  - управление инцидентами;
  - анализ функционирования СУИБ руководством организации;
  - оценка эффективности механизмов управления СУИБ;
  - другие процедуры и инструкции.

Разрабатываемые политики и процедуры должны охватывать следующие ключевые процессы СУИБ:

- управление рисками;
- управление инцидентами;
- управление эффективностью системы;
- управление персоналом;
- управление документацией и записями системы управления ИБ;

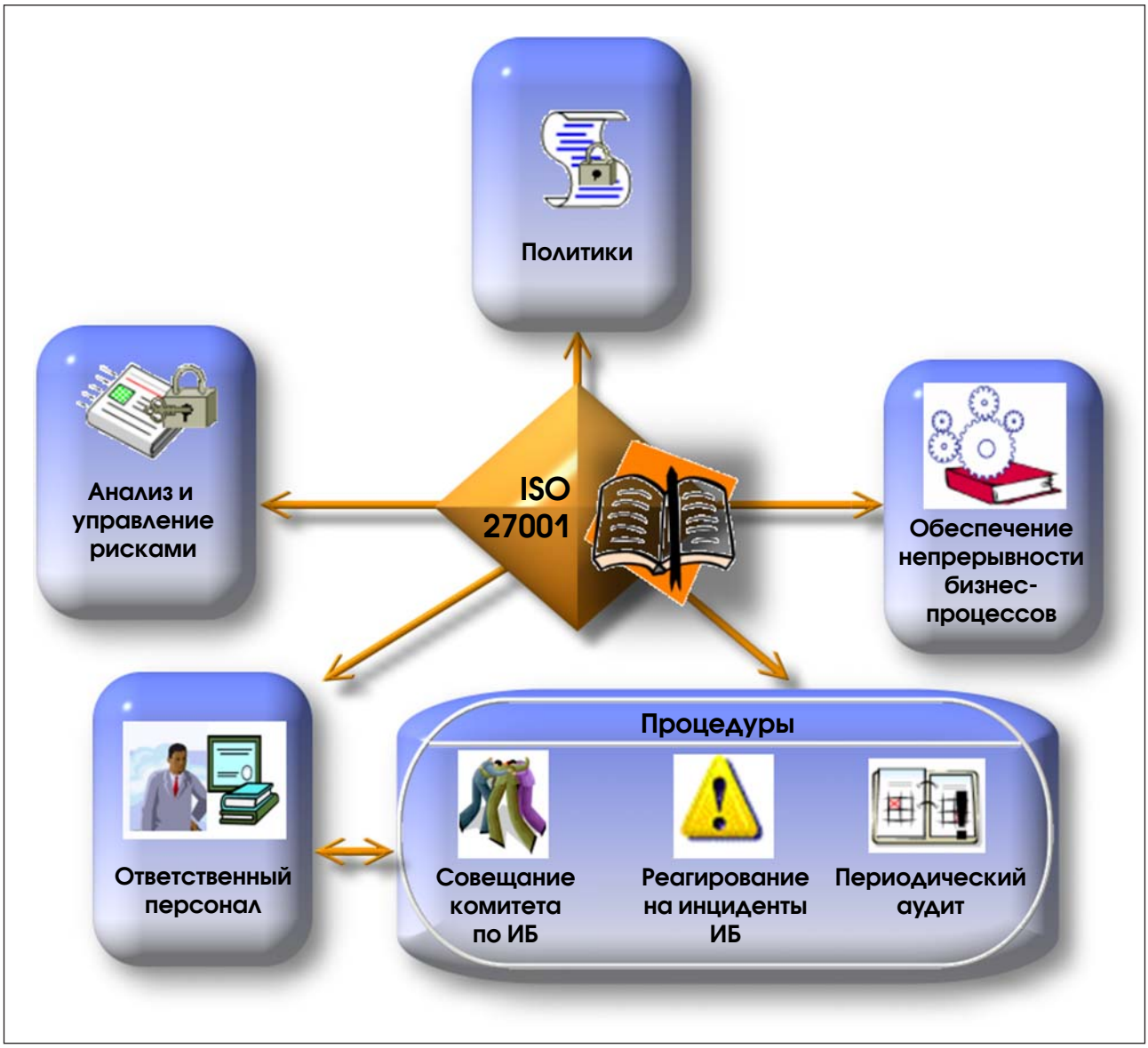

Рис.6 Основные механизмы СУИБ

- пересмотр и модернизация системы;
- управление непрерывностью бизнеса и восстановления после прерываний.

Кроме того, в должностные инструкции ответственного персонала, положения о подразделениях, контрактные обязательства организации должны быть включены обязанности по обеспечению информационной безопасности.

Обязанности по выполнению требований СУИБ посредством соответствующих приказов и распоряжений возлагаются на ответственных сотрудников подразделений, охватываемых СУИБ.

Все разработанные положения политики СУИБ, подполитик, процедур и инструкций доводятся до сведения рядовых сотрудников при их первоначальном и последующем периодическом обучении и информировании.

Таким образом, в результате не только создается документальная база СУИБ, но и происходит реальное распределение обязанностей по обеспечению безопасности информации среди персонала организации.

Внедрение СУИБ в эксплуатацию

Датой ввода СУИБ в эксплуатацию является дата утверждения высшим руководством компании положения о применимости средств управления. Данный документ является публичным и декларирует цели и средства, выбранные организацией для управления рисками. Положение включает:

- средства управления и контроля, выбранные на этапе обработки рисков (в том числе из «Приложения А» Стандарта);
- существующие в организации средства управления и контроля;
- средства, обеспечивающие выполнение требований законодательства и требований регулирующих организаций;
- средства, обеспечивающие выполнение требований заказчиков;
- средства, обеспечивающие выполнение общекорпоративных требований;
- любые другие соответствующие средства управления и контроля.

При вводе СУИБ в эксплуатацию задействуются все разработанные процедуры и механизмы, реализующие выбранные цели и средства управления (Рис.6).

Подготовка к сертификационному аудиту

На данном этапе, как и на начальном, организации рекомендуется пройти предварительный аудит, который поможет оценить готовность к сертификационному аудиту. Предварительный аудит обычно проводится тем же органом по сертификации, в котором предполагается прохождение сертификационного аудита.

По результатам предварительного аудита орган по сертификации составляет отчет, в нем отмечаются все положительные стороны созданной СУИБ, выявленные несоответствия и рекомендации по их устранению.

Для проведения сертификационного аудита рекомендуется, чтобы СУИБ компании функционировала от трех до шести месяцев. Это минимальный период, необходимый для первичного выполнения внутренних аудитов и анализа СУИБ со стороны руководства, а также для формирования записей по результатам выполнения всех процедур СУИБ, которые анализируются в ходе сертификационного аудита.

Результатом данного этапа является СУИБ организации, готовая к прохождению сертификационного аудита.

Заключение

Рассмотрев основные этапы создания СУИБ, отметим, что этот процесс достаточно сложен и длителен. Очевидно, что работы по разработке и внедрению системы не могут увенчаться успехом без ярко выраженной приверженности высшего руководства компании к созданию СУИБ. Наличие такой приверженности поможет создать эффективную и реально работающую систему.

Усилия, затраченные на создание системы управления информационной безопасностью, позволят организации выйти на новый уровень отношений с клиентами, партнерами, акционерами, продемонстрировать надежность компании и предоставят возможность успешной конкуренции с ведущими компаниями на международном рынке.

Управление инцидентами

Иван Мелехин,
старший инженер-проектировщик

Ни одна самая совершенная мера по снижению рисков информационной безопасности, будь это досконально проработанная политика или самый современный межсетевой экран, не может гарантировать от возникновения в информационной среде событий, потенциально несущих угрозу бизнесу организации. Сложность и разнообразие среды деятельности современного бизнеса предопределяют наличие остаточных рисков вне зависимости от качества подготовки и внедрения мер противодействия. Также всегда существует вероятность реализации новых, неизвестных до настоящего времени, угроз информационной безопасности. Неготовность организации к обработке подобного рода ситуаций может существенно затруднить восстановление бизнес-процессов и потенциально усилить нанесенный ущерб.

Таким образом, любой организации, серьезно относящейся к вопросам обеспечения информационной безопасности, необходимо реализовать комплексный подход к решению следующих задач:

- обнаружение, информирование и учет инцидентов информационной безопасности;
- реагирование на инциденты информационной безопасности, включая применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба;
- анализ произошедших инцидентов с целью планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом.

Также следует отметить, что при эксплуатации различного рода систем менеджмента информационной безопасности процесс управления инцидентами является одним из важнейших поставщиков данных для анализа функционирования подобных систем, оценки эффективности используемых мер снижения рисков и планирования улучшений в работе системы.

Обзор общепризнанных практик по управлению инцидентами

К настоящему времени в международной практике разработано достаточное количество нормативных документов, регламентирующих вопросы управления инцидентами информационной безопасности. Необходимо отметить, что вопрос управления инцидентами возникает не только в рамках обеспечения информационной безопасности, но и при управлении ИТ-сервисами в целом. Семейство международных стандартов ISO 20000:2005 в разделе *Service Delivery and Support* описывает ряд требований к организации процесса управления инцидентами в ИТ-инфраструктуре. Согласно данным стандартам под инцидентом понимается «любое событие, не являющееся элементом нормального функционирования службы и при этом оказывающее или способное оказать влияние на предоставление службы путем ее прерывания или снижения качества».

Специфические вопросы управления инцидентами информационной безопасности рассматриваются в следующих документах:

- **ISO/IEC 27001:2005 Information security management system. Requirements.** В рамках данного стандарта выдвигаются общие требования к построению системы управления информационной безопасности, относящиеся в том числе и к процессам управления инцидентами.
- **ISO/IEC TR 18044 Information security incident management.** Данный документ описывает инфраструктуру управления инцидентами в рамках циклической модели PDCA. Даются подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса. Рассматриваются вопросы

обеспечения нормативно-распорядительной документацией, ресурсами, даются подробные рекомендации по необходимым процедурам.

- **CMU/SEI-2004-TR-015 Defining incident management processes for CISRT.** Этот документ описывает методологию планирования, внедрения, оценки и улучшения процессов управления инцидентами. Основной упор делается на организации работы CISRT (Critical Incident Stress Response Team) — группы или подразделения, обеспечивающего сервис и поддержку предотвращения, обработки и реагирования на инциденты информационной безопасности. Вводится ряд критериев, на основании которых можно оценивать эффективность данных сервисов, приводятся подробные процессные карты.
- **NIST SP 800-61 Computer security incident handling guide.** Здесь представлен сборник «лучших практик» по построению процессов управления инцидентами и реагирования на них. Подробно разбираются вопросы реагирования на разные типы угроз, такие как распространение вредоносного программного обеспечения, несанкционированный доступ и другие.

В рамках данного обзора невозможно рассмотреть все имеющиеся рекомендации по управлению инцидентами, и вполне вероятно, что наиболее эффективным для конкретной организации будет использование какой-либо другой методологии, в том числе и разработанной самостоятельно. Но на наш взгляд, любая используемая методология должна быть совместима с основными современными стандартами на системы управления, такими как ISO/IEC 27001 и ISO 20000.

Построение процесса управления инцидентами

Международный стандарт ISO/IEC 27001 «Информационные технологии — Методы безопасности — Системы управления информационной безопасностью — Требования» вводит следующие определения:

- **событие информационной безопасности:** идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности;
- **инцидент информационной безопасности:** единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-информации и угрозы информационной безопасности

Для обработки событий и инцидентов информационной безопасности необходимо организовать процесс реагирования на инциденты. Основными задачами процесса реагирования на инциденты ИБ являются:

- координация реагирования на инцидент;
- подтверждение / опровержение факта возникновения инцидента ИБ;
- обеспечение сохранности и целостности доказательств возникновения инцидента, создание условий для накопления и хранения точной информации об имевших место инцидентах ИБ, о полезных рекомендациях;
- минимизация нарушений порядка работы и повреждения данных ИТ-системы, восстановление в кратчайшие сроки работоспособности компании при ее нарушении в результате инцидента;
- минимизация последствий нарушения конфиденциальности, целостности и доступности информации ИТ-систем;
- защита прав компании, установленных законом; создание условий для возбуждения гражданского или уголовного дела против злоумышленников;
- защита репутации компании и ее ресурсов;
- быстрое обнаружение и/или предупреждение подобных инцидентов в будущем;
- обучение персонала компании действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ.

В рамках международного стандарта ISO/IEC 27001:2005 выдвигаются следующие требования к процессу реагирования на инциденты:

Раздел 4.2.3 *Мониторинг и анализ СУИБ.*
Организация должна выполнить следующее:

- своевременно идентифицировать неудавшиеся и успешные нарушения безопасности и инциденты безопасности;

- помочь в выявлении событий безопасности и, таким образом, предотвратить инциденты безопасности путем использования индикаторов.

Приложение А. *Цели управления и средства управления.*

A.13 Управление инцидентами информационной безопасности:

- A.13.1.1 *Сообщение о событиях информационной безопасности.* Эти сообщения должны отправляться по надлежащим управленческим каналам как можно быстрее.
- A.13.1.2 *Сообщение о слабостях защиты.* Необходимо обязать всех сотрудников, подрядчиков и пользователей из сторонних организаций, использующих информационные системы и сервисы, отмечать и сообщать обо всех наблюдаемых или предполагаемых слабостях защиты систем или сервисов.
- A.13.2.1 *Ответственность и процедуры.* Должна быть установлена ответственность руководства и определены процедуры для обеспечения быстрого, эффективного и правильного реагирования на инциденты информационной безопасности.
- A.13.2.2 *Обучение на инцидентах информационной безопасности.* Должны быть реализованы механизмы, позволяющие измерять и отслеживать типы, объемы и стоимость инцидентов информационной безопасности.
- A.13.2.3 *Сбор доказательств.* Если действия, которые в результате инцидента информационной безопасности предполагается предпринять относительно лица или организации, включают в себя, кроме других, и правовые (как по гражданскому, так и по уголовному кодексу), то необходимо собрать, сохранить и представить доказательства, чтобы выполнить правила доказательства, установленные в соответствующем правоохранительном органе (органах).

Документ ISO/IEC TR 18044 Information security incident management определяет формальную модель процесса реагирования на инциденты. Целями следования этой модели является уверенность в том, что:

- события и инциденты информационной безопасности выявляются и обрабатываются эффективным образом, в особенности в части классификации событий;
- выявленные инциденты информационной безопасности в организации учитываются и обрабатываются наиболее подходящим и эффективным образом;
- последствия инцидентов информационной безопасности могут быть минимизированы в процессе реагирования на инциденты, возможно с привлечением процессов восстановления после сбоев и аварий (DRP/BCP);
- за счет анализа инцидентов и событий ИБ повышается вероятность предотвращения будущих инцидентов, улучшаются механизмы и процессы обеспечения информационной безопасности.

Процесс реагирования на инциденты состоит из следующих этапов:

- Планирование и подготовка. На данном этапе осуществляется разработка схемы реагирования на инциденты, разработка и утверждение ряда организационно-регламентирующих документов, выделение людских и материальных ресурсов, проведение необходимого обучения и апробация выбранной схемы реагирования на инциденты.
- Эксплуатация. Осуществляется обнаружение инцидента ИБ, его идентификация, предварительный анализ и начальное реагирование.
- Анализ. Проводится углубленный анализ инцидента, на его основе делаются выводы и составляются рекомендации по улучшению процесса обеспечения информационной безопасности и реагирования на инциденты. Формируется отчет об инциденте.
- Улучшение. На данном этапе реализуются рекомендации, выработанные на этапе анализа.

Рассмотрим каждый из названных этапов подробнее.

Планирование и подготовка

Данный этап является подготовительным и предназначен для организации и регламентирования деятельности по реагированию на инциденты. На этом этапе необходимо:

- выделить людские и материальные ресурсы;
- разработать схему реагирования на инциденты;
- разработать и утвердить ряд организационно-регламентирующих документов;
- провести необходимое обучение персонала и апробацию выбранной схемы реагирования на инциденты.

В соответствии с ISO/IEC TR 18044 необходимо создать группу по расследованию инцидентов ИБ. Основные цели:

- обеспечение компании квалифицированным персоналом для учета, реагирования и анализа инцидентов;

- обеспечение необходимой координации и управления процессом реагирования на инциденты;
- обеспечение должного уровня информирования руководства и заинтересованных лиц;
- обеспечение максимального снижения последствий инцидентов как в материальной сфере, так и для поддержания репутации организации.

В состав группы рекомендуется включить представителей следующих подразделений организации:

- служба информационной безопасности: обеспечение координационной, административной, экспертной и технологической деятельности;
- служба информационных технологий: обеспечение экспертной и технологической деятельности;
- служба персонала: обеспечение административной и процедурной деятельности;
- юридическая служба: обеспечение экспертной и нормативно-правой деятельности;
- бизнес-менеджеры профильных подразделений: привлекаются на временной основе для поддержки обеспечения административной, экспертной и технологической деятельности;
- внешние эксперты: обеспечение консультативной, экспертной и технологической деятельности.

Основными процессами подготовительного этапа могут быть:

- выделение людских и материальных ресурсов;
- разработка и утверждение организационно-распорядительной документации;
- обучение персонала;
- тестирование схемы реагирования на инциденты.

Эксплуатация

На данном этапе осуществляются обнаружение инцидента ИБ, его идентификация, предварительный анализ и реагирование на инцидент.

Основные процессы этапа:

- обнаружение и идентификация инцидента;
- предварительный анализ инцидента;
- начальное реагирование на инцидент;
- реагирование на инцидент.

Анализ

Группа по реагированию на инциденты проводит углубленный анализ инцидента, на основе результатов анализа делаются выводы и составляются рекомендации по улучшению процесса обеспечения ИБ и реагирования на инциденты. Формируется отчет об инциденте.

Основным процессом этапа является углубленный анализ инцидента.

Улучшение

На данном этапе осуществляется реализация рекомендаций по улучшению процессов обеспечения ИБ и реагирования на инцидент. Утвержденные уполномоченным лицом компании рекомендации передаются на исполнение ответственным лицам.

Обобщенная схема процессов управления инцидентами приведена на рис. 1. (Стр. 18).

Автоматизация процессов управления инцидентами

При автоматизации процессов управления инцидентами в первую очередь необходимо уделять внимание автоматизированной обработке событий информационной безопасности — основе практически любого инцидента. События от различных технических средств защиты являются важнейшим поставщиком информации о процессах, происходящих в системе управления информационной безопасностью (СУИБ), нарушениях, рисках. На основании событий проводится корректирующие действия, оценка текущей защищенности системы, эффективности функционирования СУИБ. Только обладая полным и достоверным набором событий, можно провести надлежащее расследование инцидентов, получить представление о динамике развития СУИБ. Можно сказать, что события — основной канал обратной связи для управляющих воздействий в рамках СУИБ. Немаловажным является и то, что события легко документируемы и воспроизводимы.

Организация процесса обработки событий без использования средств автоматизации представляет собой сложную и трудоемкую задачу. Необходимо собирать и консолидировать большое количество данных в различных форматах, вести центральный архив. Для ручной обработки

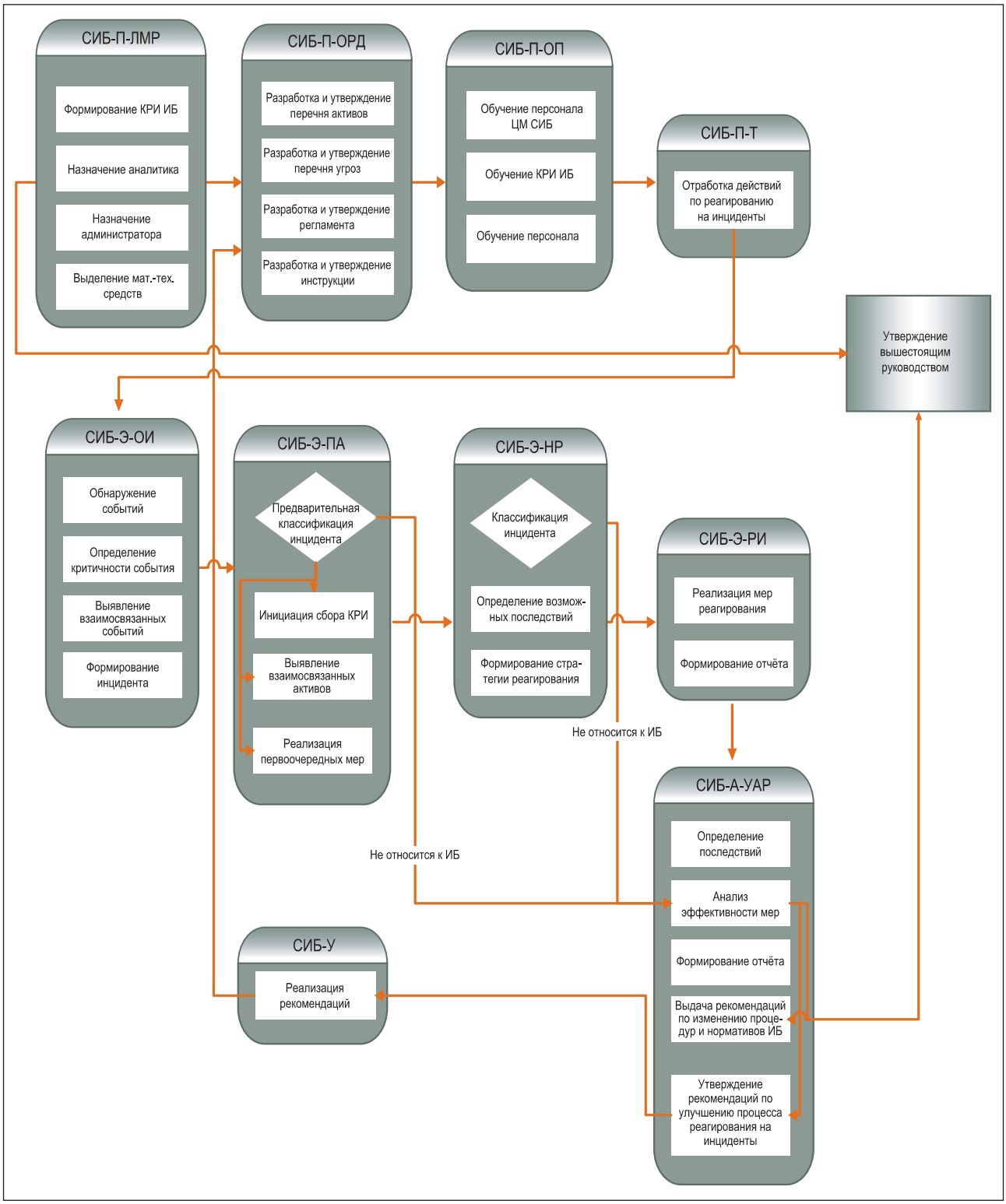

Рис. 1. Схема процессов управления инцидентами

событий требуется большое число высококвалифицированных специалистов – аналитиков. В силу большого объема рутинной ручной работы обработка событий зачастую бывает неполной, не отражающей всю полноту текущей ситуации. При этом возможна ситуация, когда события, критичные для надежного и защищенного функционирования бизнес-систем, окажутся вне поля зрения аналитиков, и в отношении них не будут приняты соответствующие превентивные меры.

Для поддержания процесса обработки событий на уровне, соответствующем современным тре-

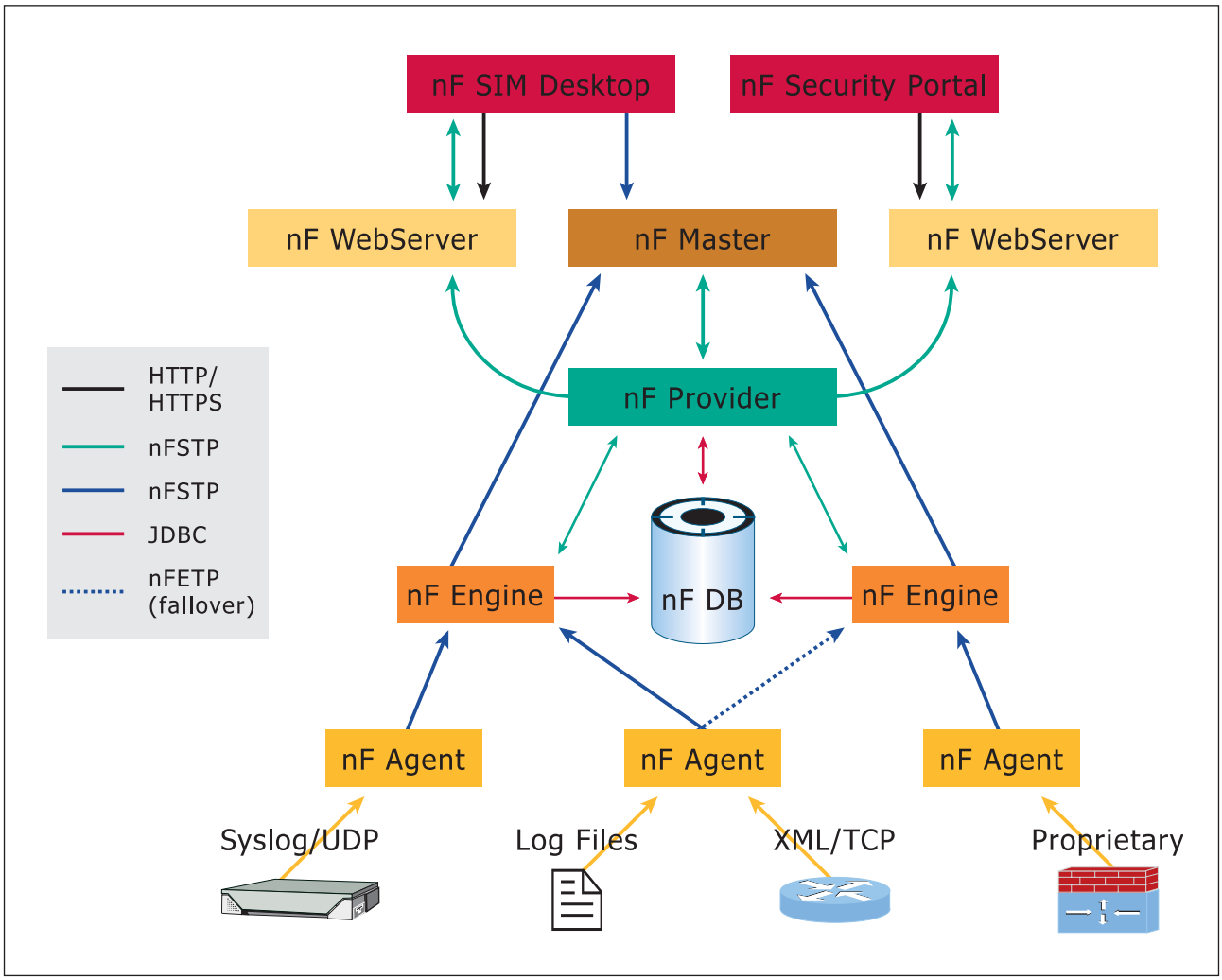

Рис. 2. СУИБ netForensics

бованиям, возможно применение различных автоматизированных систем обработки событий (СОС).

СОС должны обеспечивать следующий функционал:

- позволять собирать события от всех технических средств обеспечения защищенности, используемых в рамках СУИБ;
- производить нормализацию событий, приводя их к единому формату;
- осуществлять хранение событий способом, позволяющим хранить необходимые объемы данных;
- предоставлять инструментарий для поиска в хранилище данных;
- предоставлять механизмы формирования отчетов различного рода;
- СОС должна быть расширяемой и масштабируемой;
- опционально осуществлять корреляцию собранных событий.

Процесс обработки событий автоматизированными системами включает следующие основные шаги: нормализация (приведение к единому формату) данных, агрегирование (накопление), корреляция и визуализация. На первых двух стадиях информация о событиях безопасности собирается практически со всех используемых в рамках СУИБ средств защиты: межсетевых экранов, систем обнаружения атак, антивирусных систем, операционных систем и приложений различных производителей, средств контроля физического доступа, и преобразуется в единый, удобный для понимания формат. Собранные данные подвергаются корреляции и выводятся на консоль оператора системы.

Развитые средства поиска позволяют проводить оперативное и всестороннее расследование инцидентов, обеспечивать свидетельства наличия и функционирования средств защиты в рамках СУИБ при проведении различных аудитов.

В настоящий момент на рынке присутствуют автоматизированные системы, реализующие требуемый функционал. Компания «Инфосистемы Джет» использует в своих решениях программный продукт для обработки событий — netForensics nFX Open Security Platform. (Рис.2).

Система управления информационной безопасностью netForensics предназначена для работы с гетерогенной средой продуктов обеспечения информационной безопасности и реализует непрерывный сбор, обработку и отображение событий безопасности. Система работает под управлением ОС Windows, Linux или Solaris, используя в качестве хранилища данных полнофункциональную СУБД Oracle. Описываемая СУИБ имеет широкие возможности работы в распределенном режиме, поддержку различных отказоустойчивых конфигураций. Система netForensics реализована на базе технологии Java по модульному принципу.

Основные модули системы:

- сервер приложений — реализует основную логику обработки событий, представления данных, взаимодействия с пользователями;
- база данных — обеспечивает хранение поступающей в систему информации;
- модуль корреляции — осуществляет корреляцию собранных данных;
- модуль автоматизации управления инцидентами — осуществляет автоматизацию процессов управления инцидентами;
- агенты — собирают информацию непосредственно с устройств.

В состав системы входят средства для написания агентов сбора данных с нестандартных средств защиты, средства задания пользовательских правил корреляции и создания отчетов.

Заключение

Эффективно организовав и внедрив процесс управления инцидентами, компания получит следующие бизнес-преимущества:

- снижение отрицательного влияния инцидентов на бизнес организации;
- доступность необходимой для бизнеса управленческой информации;
- превентивное определение мер по улучшению информационной защищенности.

Правильно организованный процесс управления инцидентами в подразделениях службы информационной безопасности это:

- четкое определение для всех специалистов ролей и ответственности за качественное и своевременное реагирование на инциденты;
- оперативная информация для мониторинга эффективности принимаемых защитных мер;
- прозрачность контроля за эффективностью работы сотрудников подразделения;
- повышение качества взаимодействия специалистов в смежных ИТ- и бизнес-подразделениях.

Система автоматизации процесса управления инцидентами дополнительно позволит:

- обрабатывать и хранить информацию о событиях и инцидентах информационной безопасности, а также обо всех действиях по их устранению;
- оперативно принимать решение по устранению возникшего инцидента, основываясь на анализе информации о предыдущих инцидентах;
- проводить анализ накопленных данных.

Контентная фильтрация: разбор объектов информационного обмена

Олег Слепов,
консультант по информационной безопасности

Под контентной фильтрацией понимается фильтрация содержимого информационного обмена по каналам Интернет (электронная почта, веб, интернет-пейджеры типа ICQ, MSN и т.п.). Фильтрация предполагает рекурсивную декомпозицию (разбор или распаковку) объектов информационного обмена, их анализ (то есть установление по определенным признакам соответствия с заданными шаблонами) и выполнение действий над ними по результатам такого анализа.

На рынке появилось много средств контроля содержимого информационного обмена по каналам Интернет. Существующие системы в большинстве своем не способны обеспечить качественный разбор объектов информационного обмена.

Практика показала, что наиболее проблематичным этапом контентной фильтрации является декомпозиция объектов. Основная причина состоит в их сложности, которая заключается в следующем:

1) множественность кодировок в различных частях объектов информационного обмена;
2) широкий круг задач, которые выполняют информационные системы (это обстоятельство привело к появлению разнообразных приложений и прикладных программ, что в свою очередь стало причиной большого количества новых форматов данных и файлов различных типов; сейчас тенденция такова, что новых форматов и типов данных будет появляться все больше);
3) сами файлы стали представлять собой сложную структуру, включающую большое количество уровней вложенности, а также различные другие инкапсулированные компоненты; например, современные файлы MSOffice содержат в себе OLE-объекты[1]; объектом может быть целый файл или только фрагмент файла, графические объекты, тексты, фрагменты звукозаписи и видеозаписи.

Представленные на рынке средства контентной фильтрации не учитывают сложность и комплексность объектов информационного обмена. К сожалению, основной упор в данных системах делается на категоризацию объектов, то есть анализ содержимого и присвоение ему некоторой категории из предварительно составленного списка. И совсем не принимается во внимание, что если объект не разобран, невозможно провести анализ его содержимого.

Кроме того, часть имеющихся на рынке систем определяют формат данных и кодировку текстов только по mime-типу[2], указаному в служебных заголовках. Mime-тип присваивается приложением, в котором создан объект. Приложения далеко не всегда верно указывают mime-тип, что приводит к ошибкам при разборе.

Часть существующих решений по определению типов данных в средствах контентной фильтрации построены на базе широко известной утилиты file и библиотеки libmagic. Для этой

1 Связь и внедрение объектов, созданных в различных приложениях, осуществляются в Windows с помощью специальной технологии, которая называется OLE (Object Linking and Embedding — связь и внедрение объектов). Технология OLE — это универсальный механизм для создания и обработки составных документов, содержащих одновременно объекты различного происхождения, разной природы, например, текст, таблицы, фотографии, звук и т.п.
Технология OLE позволяет:

- внедрять в документ объекты или фрагменты документов, созданные в других приложениях, а также редактировать эти объекты средствами создавшего их приложения;
- устанавливать связь объекта с документом другого приложения. При установлении связи этот объект продолжает «жить» собственной жизнью и обслуживать другие документы.

2 mime-тип — это стандарт, который определяет систему названий типов данных.

утилиты имеется большая база сигнатур для разных типов данных.

Однако эта система обладает недостатками, наиболее существенным из которых является отсутствие гибкого языка описания проверок типов данных. В результате возникают серьезные ошибки при распаковке объектов информационного обмена (это может быть неправильное определение мультимедиа или исполняемых файлов) и/или невозможность анализа сложных объектов (например, файлов Microsoft Office). File допускает такие ошибки: некоторые mp3-файлы определяются как текстовые. Mp3-файлы позволяют вставлять текстовые фреймы в свои произвольные участки, file цепляется за эти участки и ошибается при определении типа.

У file бывают проблемы с файлами маленькой длины. Например, если текстовый файл с одним словом, то при совпадении по буквам с бинарным кодом file может определить это слово как бинарный код. Причем если этот файл был в архиве, то архив может быть полностью вырезан.

Еще одна проблема — определение кодировки. Большинство присутствующих на российском рынке систем производятся в Европе или Северной Америке. В странах этих регионов стандартизации с самого начала отводилась важная роль, поэтому там изначально не было проблем с множественностью кодировок. А поскольку кодировка одна, то ее определению не придавалось большого значения. К сожалению, по тому же пути пошли и многие российские разработчики.

Почему же важно правильно определять кодировку текста?

Во-первых, в России, странах СНГ, а также во многих государствах Азии множественность кодировок — это проблема. В России и странах СНГ язык один — русский (или другой национальный, например, украинский), кодировок — пять. В Азии: язык один — японский, кодировок — три-четыре.

Во-вторых, без определения кодировки невозможно решение большинства бизнес-задач. Многие компании имеют свои отделения в других странах. Например, у европейского банка могут быть отделения в странах Азии. Как правило, центральные офисы таких компаний получают входную информацию в национальных кодировках. Система контентной фильтрации должна иметь возможность обслуживать трафик одновременно на нескольких языках.

Эти потребности и определяют тенденции развития контентной фильтрации в будущем: разбор объектов информационного обмена в настоящее время выходит на передний план.

Подход компании «Инфосистемы Джет»

Разработчики компании «Инфосистемы Джет» учли перечисленные выше недостатки аналогичных систем контентной фильтрации. В своих решениях они главное внимание уделяют вопросу разбора объектов на составляющие компоненты. Если объект разобран правильно, то его просто анализировать.

В линейке продуктов «Дозор-Джет» упор делается на надежное определение типов данных и гарантированное определение кодировки текстов. Это в итоге позволяет добиться высокой эффективности фильтрации.

Компания «Инфосистемы Джет» определила свой подход к данной задаче: любой объект информационного обмена по каналам Интернет изначально рассматривается как композитный. То есть в него могут входить различные компоненты: текст, файлы, закодированные бинарные данные, описания и комментарии. Предполагается, что каждый входящий в такой объект компонент в отдельности также может быть сложным объектом.

Определение типов файлов осуществляется не по mime-типу, поскольку этот mime-тип может быть неверно определен. Гарантированное определение типа файла возможно только по его бинарному следу.

Определение кодировки состоит из двух этапов. Первым этапом является определение языка. Затем в рамках языка эмпирически определяется кодировка. Любой язык имеет некие законы построения слова. Любой связный текст обладает определенными характеристиками. Именно эти законы и характеристики ложатся в основу определения кодировки текста в решениях компании «Инфосистемы Джет».

Надежное определение типов данных и языковых кодировок обеспечивается в линейке продуктов контентной фильтрации компании «Инфосистемы Джет» за счет применения уникального программного комплекса определения типов данных.

Программный комплекс определения типов данных

Сегодня существующие на рынке информационной безопасности решения по определению типов данных имеют целый ряд недостатков, среди которых:

- слабые возможности языков описания проверок типов данных;

- слабая расширяемость;
- невозможность анализа сложных объектов;
- сложность сопровождения баз mime-типов.

С учетом этого в 2005 году специалистами компании «Инфосистемы Джет» был разработан новый комплекс определения типов данных. По своей сути комплекс является know-how компании. По техническим характеристикам он превосходит все имеющиеся на ИТ-рынке аналогичные системы. В основе данной разработки лежит громадный опыт внедрений систем контентной фильтрации.

По сравнению с другими аналогичными системами на рынке средств контентной фильтрации система по определению типов текстовых файлов работает более корректно. Анализатор текстовых файлов позволяет производить в них поиск данных, закодированных в различных форматах. Здесь представлены некоторые из них: Plain Text, HTML, SMGL, Microsoft Word, Microsoft Excel, Microsoft Help Data, Microsoft Compressed Help Data, Microsoft Access Database, TNEF, RTF, PDF, Postscript, Power Point, Base64, Uuencode, Quoted-Printable и т.д.

Кроме того, в системе «Дозор-Джет» как для выдачи текстового описания типа, так и для выдачи mime-типа используется одна база условий. А это позволяет избежать ошибок, которые могут возникнуть при ведении двух аналогичных баз данных.

Гарантированное определение кодировки в системе «Дозор-Джет» обеспечивается за счет эвристического анализа текстов, поэтому удается успешно проводить анализ текстов с неверно указанной кодировкой. А самое важное, что «Дозор-Джет» позволяет определять кодировки в текстах внутри архивированных файлов.

Описанная выше функциональность «Дозор-Джет» стала возможной за счет:

- наличия специализированного языка описания проверок типов данных;
- возможности расширения языка проверок;
- возможности подключения модулей анализа;
- явного отображения сигнатур в mime-типы.

Язык описания условий проверки сигнатур

Самым главным достоинством новой системы является мощный язык описания условий проверки сигнатур. Благодаря этому языку стал возможным более глубокий анализ сложных объектов (файлы mp3 и .exe). А для случаев, когда анализ трудно описать на встроенном языке, существует возможность создания подгружаемых модулей анализа.

Встроенный язык описания проверок обеспечивает анализ разных типов данных (числа, строки, символы, списки), а также позволяет применять к ним разные операции:

- операции сравнения;
- арифметические операции;
- битовые операции;
- логические операции;
- прямая и косвенная адресация проверяемых данных;
- условные операторы;
- форматированный вывод.

С помощью данной системы можно описывать более сложные условия проверки типов данных, таких как:

- проверка значений (байты, строки, целые числа) по заданным смещениям с помощью условий <,>,= и их сочетаний;
- вычисление значений и смещений с использованием арифметических и битовых операций, что позволяет использовать косвенную адресацию данных;
- проверка размера файла;
- комбинирование условий проверки с помощью логических операторов;
- использование условных операторов для проверки конкретных значений;
- уточнение типов с помощью модулей расширения.

Дополнительные модули анализа данных

При уточнении типов данных и/или проведении глубокого анализа инфраструктура системы позволяет использовать модули расширения. В настоящее время реализованы следующие модули анализа данных:

- модуль определения текстов и методов их кодирования (ASCII, EBCDIC); важность его определяется тем, что для текстовых файлов не существует сигнатур, по которым можно определять типы;
- модуль определения исполняемых файлов MS-DOS – .com-файлы; как и для текстовых, для таких файлов не существует стандартных сигнатур, поэтому необходимо проводить детальный анализ содержимого файлов;
- модуль определения главного типа OLE-контейнера – MS Visio, MS Project, MS Word, MS Excel, MS Powerpoint.

Проблемы управления средствами ITSEC в больших компаниях

Борис Тоботрас,
начальник отдела защиты телекоммуникаций
Дмитрий Михеев,
инженер отдела защиты телекоммуникаций

Компания «Инфосистемы Джет» уже более 10 лет проводит работы по информационной безопасности (ИБ). За это время успешно реализовано более 300 проектов по защите информации в федеральных и муниципальных структурах, банках и финансовых учреждениях, крупных торговых и промышленных предприятиях. Основываясь на многолетнем опыте внедрения систем безопасности, в том числе и собственных продуктов по ИБ, специалисты компании «Инфосистемы Джет» разработали идеологию управления средствами ITSEC в больших системах, которой и руководствуются в повседневной деятельности.

Под большими системами в данном случае подразумеваются крупные информационные сети как по размерам и территориальной распределенности, так и по масштабам решаемых с их помощью задач. Такие системы, как правило, охватывают значительные человеческие ресурсы, объединяют различные организации, включают массу разнообразных систем и оборудования. Необходимо иметь в виду, что построение этих систем происходило не за один день, а входящие в них компоненты создавались на различных этапах развития ИТ-индустрии, а значит, изначально могли иметь фундаментальные структурные различия.

Цель данной статьи — обобщить и сгруппировать все проблемы, связанные с управлением средствами ITSEC в больших информационных системах, и наметить пути их решения.

Задачи управления средствами ITSEC в больших системах

Для того чтобы иметь возможность решать сложные задачи по построению интегрированных систем безопасности, необходимо провести тщательную классификацию проблем, возникающих при их построении. Такая классификация поможет определить, какие же задачи управления средствами ITSEC являются актуальными в настоящий момент в больших и распределенных информационных системах.

Как это ни покажется странным на первый взгляд, основной проблемой больших сетей является их размер. Сложные сетевые конфигурации, требования к безопасности и надежности — в больших системах все эти проблемы принимают глобальные масштабы.

Сложные сетевые конфигурации

Инженерам центра информационной безопасности компании «Инфосистемы Джет» в своей практике часто приходится сталкиваться с построением сложных сетевых конфигураций. На основании нашего опыта можно говорить о нескольких основных проблемах.

Рассмотрим некоторые из них.

Структура сети

Одной из часто возникающих задач является преодоление проблем, связанных с сетевой трансляцией адресов. Пример: если надо обеспечить соединение из центра к управляемому объекту в локальной сети, подключенной через NAT, то потребуется искать обходные пути либо дорабатывать конфигурацию NAT, так как в простом варианте соединение будет блокировано. Приходится усложнять схему настройки, править политики доступа. Система управления должна нормально работать в таких условиях, так как они крайне распространены. Вариантом решения может быть инициация запроса с клиентской стороны.

Сходной проблемой является отсутствие карты сети с указанием существующих сегментов, а также планов развития сетевой инфраструктуры. При подготовке любых работ на сети необходимо большое количество информации по различным аспектам — адресация, маршрутизация, физические соединения, информационные потоки, статистика по загрузке и другие показатели.

Как правило, не составляет трудностей получение подобной информации по какому-либо конкретному объекту системы. Составление же общей картины, хотя бы в виде ответов на конкретные вопросы, может оказаться более сложной задачей. Часто для внедрения систем безопасности требуются выделение подсетей стыка, модификация маршрутизации, а подобные изменения требуют серьезной подготовки и вмешательства в ряд элементов системы. Выделение адресного пространства, как правило, требует времени и объединенных усилий многих специалистов.

Различные скорости связи

Серьезные проблемы при построении интегрированных систем безопасности возникают в связи с различием скоростей передачи данных на разных участках информационных систем. Например, информационная система компании состоит их двух локальных вычислительных сетей, объединенных в одну инфраструктуру и связанных между собой определенным каналом связи. Каждая из этих сетей создана таким образом, чтобы обеспечивать быстрый и качественный обмен данными. Однако образованный между ними канал не способен обеспечить быструю связь. Происходить это может потому, например, что между локальными сетями лежит старый E1 или спутниковый канал, который, может быть, и не очень медленный, но вносит свои особенности из-за свойственных данному виду связи задержек.

Очень узким местом являются используемые до настоящего времени dial-up каналы. В некоторых случаях используются мобильная связь и wi-fi, которые в настоящее время не обладают достаточной скоростью передачи данных. Широко распространенные сейчас в некоторых регионах ADSL каналы могут принести проблемы из-за разницы ширины канала в разных направлениях. Применение для авторизации различных вариантов туннелирования вызывает проблемы с совместимостью устройств.

Наличие узких каналов связи порой приводит к ухудшению качества работы системы в целом. Так, система управления может использовать определенную полосу для своих нужд — пересылки разного рода сообщений, журнальных записей, служебных соединений. Система, рассчитанная на стабильную работу в сетях 100мбит/с, иногда плохо работает на более узких каналах либо создает загрузку, мешающую бизнес-процессам.

Совместимость и способность к миграции

Сейчас программное обеспечение разрабатывается с очень коротким циклом выпуска, а современные угрозы требуют постоянного ответа на уязвимости. Быстрое обновление поколений продуктов в сочетании с размерами сетей и требованиями по производительности и надежности приводят к необходимости последовательного обновления программного и аппаратного обеспечения. Учитывая, что в большой сети не всегда можно произвести полномасштабное обновление за короткий период времени, определяются требования к совместимости продуктов между собой. Обеспечение таких возможностей требует значительных усилий по моделированию ситуаций, отработке надежных сценариев миграции и высокой квалификации специалистов. В продуктах собственной разработки наша компания закладывает возможности по миграции и совместимости отдельной задачей.

Серьезной задачей является также поддержание ПО на должном уровне — наложение патчей, обновления баз и т.д. В больших корпоративных сетях эти возможности крайне востребованы и необходимы для нормального управления подсистемой безопасности.

Диалектика развития больших сетей

Все сети когда-то были маленькими. Большими они стали не за час, не за год, а за десятилетия. Современные информационные системы продолжают опираться на достаточно развитую инфраст-

руктуру — электрические, кабельные, телефонные сети, спутниковые сегменты, которые также продолжают развиваться. За прошедшие годы несколько раз менялись поколения техники и технологий связи.

Развитие информационных сетей продолжается, причем достаточно интенсивно, и есть все основания считать, что этот процесс в России будет таким и в ближайшем будущем.

Широкий парк оборудования

Характерной особенностью больших сетей является наличие огромного количества аппаратно-технических средств. Они различаются не только по производителю и характеристикам, но и по платформам и технологиям. Объясняется это несколькими причинами: аппаратура приобреталась в разное время; закупки и внедрение могли производиться разными специалистами, которые не только имеют свои предпочтения, но и по-разному видят построение информационной сети. В результате последовательного роста сетей из малых в большие в них образовались своеобразные «годовые кольца», определенные наслоения. Разумеется, все это внесло неразбериху и создало серьезные проблемы для внедрения систем информационной безопасности.

Гетерогенные системы

Объединение разных систем в одно целое выявляет специфические проблемы совместимости, исходящие от разных платформ, версий ОС, версий прикладного программного обеспечения.

С практической точки зрения это означает, что необходимо держать библиотеку отработанных решений по интеграции этих технологий. Инженеры нашей компании подобный опыт имеют, и это позволяет нам успешно работать, например, с почтовыми системами, включающими в себя одновременно MS Exchange, Lotus Notes, sendmail, LDAP и целый набор антивирусного обеспечения, обрабатывающие протоколы SMTP, MAPI, и другие, менее распространенные. Достигается это планомерной работой в области развития нашего собственного ПО, доработкой свободного ПО силами наших специалистов, а также серьезными усилиями по документированию подобных решений.

Недостаток контроля

При запуске оборудования или ПО от них в первую очередь требуется выполнение основной функции. Все остальные функции могут быть оставлены на потом или не использованы вообще. Системы журналирования, оповещения, удаленного управления и, как ни странно, безопасности, как правило, страдают от такого отношения к делу.

Кроме того, из-за растянутости во времени процесса развития сети с привлечением разных специалистов могут возникать ситуации, когда у владельца сети теряется или радикально меняется понимание логики организации отдельных ее элементов. Возникают «медвежьи углы», о которых никто из актуальных сотрудников не имеет представления.

В результате процесс внедрения любой системы приводит к необходимости всестороннего исследования инфраструктуры и информационных потоков, не гарантируя стопроцентного отсутствия проблем. Так, например, после установки МЭ в большой сети с написанием развернутой политики безопасности и запуска всего этого в работу, может оказаться, что в той же сети уже год работает VoIP-сервис, широко используемый одним из клиентов владельца сети. Это требует значительных изменений в работах, оборудовании и ПО для продолжения нормального функционирования сети. При этом, следует отметить, никто из сетевых инженеров заказчика не знал о подобной ситуации, при проектировании политики МЭ данный сервис учтен не был и оказался недоступен в течение нескольких часов.

Полностью застраховаться от подобных ситуаций невозможно. Владелец сети по определению знает о ней больше, чем приглашенный консультант, по крайней мере, до проведения исследования. Как-либо минимизировать данную проблему позволяет исключительно планирование и документирование сетевой инфраструктуры, в чем у нашей компании накоплен значительный опыт. Наличие подробного плана сети с документально закрепленными зонами ответственности, явно документированной и согласованной стратегией развития является редкостью. Без такой подготовки практически любое серьезное вмешательство в инфраструктуру (а внедрение любого вида средств безопасности в работающую сеть является достаточно болезненным мероприятием) приведет к большому количеству проблем.

Размывание зон ответственности

Описанное выше «многообразие» больших и распределенных информационных сетей приводит к размыванию зон ответственности. Во-первых, разные части сети находятся в разном администт-

ративном подчинении и могут развиваться без учета «общей картины мира». Во-вторых, в больших сетях каждый администратор, как правило, знает только свою часть сети, в то время как пограничные участки, лежащие на стыках, могут быть им неизвестны. Это приводит к возникновению «белых пятен на карте» информационной сети, а значит, к серьезным уязвимостям в информационной безопасности.

Банальным примером является объединение двух сетей с пересекающимся диапазоном IP-адресов. С этим регулярно приходится сталкиваться специалистам компании «Инфосистемы Джет» у своих заказчиков.

Отсутствие «общей картины мира»

Другим важным моментом является то, что получить «общую картину мира» из одного источника практически никогда не удается. Разные зоны ответственности, отсутствие сформулированной в документах и руководствах идеологии построения и развития системы приводят к тому, что нет общего понимания происходящего.

При попытке работать на стыке нескольких зон ответственности, как обычно бывает со средствами безопасности, возникают характерные проблемы, основной из которых является неопределенность последствий. Из-за непонимания происходящих в сети событий невозможно предсказать результат изменений. К сожалению, надо быть готовым приостановить внедрение из-за вскрытия новых обстоятельств, исследовать все подробнее и выработать новую последовательность действий. В нашей работе приходится порой откладывать в сторону текущую задачу, чтобы разобраться в ситуации. В противном случае в будущем можно столкнуться с еще большими проблемами.

Географическая распределенность

Большинство современных больших систем являются географически распределенными сетями. Они находятся уже не только в разных городах, но и странах, и даже на различных континентах. Для взаимодействия и обмена данными в таких системах применяются каналы от Интернета до собственных каналов радиорелейной и спутниковой связи.

Это приводит к необходимости держать большой штат инженеров для реагирования на проблемы, требует изрядных ресурсов на внедрение, усложняет задачи снабжения оборудованием и комплектующими. Кроме того, из-за этого увеличивается время устранения проблемы, что отрицательно влияет на отношения с заказчиком и вредит компании.

Распределенность по временным зонам

Географическая удаленность различных объектов инфраструктуры больших сетей автоматически тянет за собой проблему распределения по часовым поясам. Разница во времени приводит к сложностям в координации усилий. Становится проблематичным согласованное переключение оборудования, трудно использовать телефонные переговоры. Отсутствие специалистов на любой из двух сторон может создавать проблемы.

Например, во Владивостоке в момент подготовки презентации в 12 часов местного времени возникает проблема, в Москве это 19 часов, и уже может не быть на месте специалиста, способного помочь. Если у вас есть журналы с двух устройств, расположенных в разных временнных зонах, насколько свободно вы сможете сказать, что событие А в одном журнале соответствует событию Б в другом журнале?

Неполное функционирование системы в каждый конкретный момент

Из-за большого количества аппаратно-технических средств, распределенных географически в разных часовых зонах, проистекает также вероятность того, что часть оборудования, в том числе системы безопасности, не будет полностью функционировать в определенный момент времени. К примеру, при загрузке политики на устройства централизованно из единого центра управления существует необходимость в установлении устойчивой связи со всеми удаленными площадками и объектами. Если хоть один из каналов связи будет блокирован, данная операция может привести к разного рода проблемам.

Возможность возникновения подобных ситуаций необходимо учитывать. Соответственно, система управления средствами и системами защиты должна уметь определить такую ситуацию, исправить ее или иным образом обеспечить выполнение поставленной задачи.

Кроме того, масштаб проводимых работ и различие по подчинению практически исключают одновременность событий. В таких системах возможно развитие только через серию последовательных изменений.

Требуемые свойства инфраструктуры управления

Состояние современных больших и распределенных систем, условия их эксплуатации, а также постоянно возникающие проблемы их функционирования предъявляют определенные требования к их безопасности. Во-первых, они должны «выдерживать» радикальные изменения направлений развития. Во-вторых, должны быть достаточно гибкими для работы в таких условиях и позволять контролировать свое поведение в описанных выше условиях эксплуатации. Даже если произойдет смена концепции информационной системы (что бывает нередко), комплекс информационной безопасности должен работать надежно и без сбоев, выполняя свою основную задачу, а именно обеспечивать:

- конфиденциальность информации, то есть защиту от несанкционированного доступа (НСД) и других способов нелегального ознакомления;
- целостность информации, то есть ее достоверность, полноту и актуальность;
- доступность информационных сервисов, то есть возможность получения информации за время, предусмотренное нормативными, техническими и иными требованиями.

Требования к гибкости

Наличие сетей со сложной конфигурацией приводит к повышению требований, предъявляемых к гибкости продуктов безопасности и систем управления. Как показала практика, даже очень хорошо работающая система информационной безопасности при ее внедрении в какую-нибудь сложную сеть может оказаться в ситуации, когда ее возможности описания конфигурации недостаточно.

У каждого производителя систем безопасности существует определенное представление того, как будут использоваться его продукты. Однако это представление не всегда совпадает с действительностью. Опыт показывает, что многие продукты не обладают гибкостью и не могут без проблем интегрироваться в сети со сложной конфигурацией.

Поскольку «Инфосистемы Джет» сами являются производителем средств защиты и одновременно с этим — системным интегратором в области информационной безопасности, специалисты компании выработали свое видение данной проблемы. Наши разработчики не просто адаптируют свою продукцию при внедрении в сети со сложной конфигурацией, но уже при проектировании продуктов безопасности закладывают некоторый простор по гибкости и возможности развития продукта в будущем. Накопленный опыт проектирования, внедрения и длительного сопровождения крупных инсталляций в области серверных комплексов, сетевой инфраструктуры и систем безопасности, опыт проведения аудита и работы с системами различных поставщиков позволяют нам предвидеть возможные проблемы и находить решения данных ситуаций.

Разработчики программного обеспечения заботятся о возможности расширения в дальнейшем форматов передачи данных, конфигурационных файлов в наших продуктах. Для решения этих проблем готовятся и тестируются средства миграции и диагностики.

Критичное отношение к результатам работы побуждает фиксировать и разбирать проблемы, возникающие на реальных внедрениях.

Неизбежность последовательных изменений

Отличительной особенностью больших систем является то, что невозможно производить какие-либо изменения, отключив, например, всю сеть. При проведении работ по модернизации или обслуживанию систем безопасности не избежать последовательных изменений. Это значит, что такие изменения должны производиться поочередно в отдельных сегментах сети, шаг за шагом продвигаясь дальше, учитывая все сложности, описанные в предыдущих главах.

Информационные системы сегодня представляют собой один из значимых активов практически любой компании. Ценность накопленных данных, масштаб проникновения в бизнес-процессы трудно переоценить. Вряд ли идея полного отключения информационной системы расчетных центров любого банка для проведения обновления ПО найдет горячих поклонников.

Кроме того, последовательность изменений является следствием распределения зон ответственности.

Распределение зон ответственности

Неясность зон ответственности, о которой говорилось в предыдущих главах, приводит к необходимости обеспечения высокой степени координации управления системами безопасности, находящимися в различных частях, и сегментами

больших сетей. При этом должно учитываться ограниченное количество ресурсов управления и специалистов, эксплуатирующих данные системы. Необходимо иметь в виду, что за отдельные участки системы отвечают различные люди, и такая распределенная ответственность не должна стать препятствием на пути реализации задачи внедрения и управления средствами ITSEC в больших сетях.

Для данной проблемы не существует однозначного решения. Общая дисциплина и прописанные взаимоотношения между субъектами могут облегчить работу, но окончательно ее не снимут. Спектр возможных отношений партнерства, подчинения и влияния между субъектами в сложных системах очень широк, и задачей средств безопасности в этой ситуации является максимальная гибкость.

Опыт крупномасштабных проектов в различных областях, значительный экспертный потенциал, высокий уровень подготовки инженеров позволяют минимизировать отрицательные эффекты таких ситуаций, но полностью их избежать нельзя.

Возможность отката изменений

Всегда при выполнении изменений существует вероятность, что новое состояние будет хуже прежнего. Ошибка, проявившаяся на данной конфигурации, неучтенная особенность, человеческий фактор, повышенные требования к производительности платформы у новой версии — все это может вызвать вместо ожидаемого улучшения ухудшение ситуации.

Следует обращать внимание на подобные ситуации, планировать варианты отката изменений, собирать и обобщать данный опыт во избежание подобного в будущем.

Высокие требования к надежности и доступности

Надежность системы

В больших сетях, как, впрочем, и в любых других, всегда предъявляются очень высокие требования к надежности функционирования системы и доступности данных. Это изрядно ограничивает действия по управлению средствами и системами безопасности. В действительности часто нет возможности, например, остановить функционирование серверного комплекса, чтобы провести профилактическую работу. И наоборот, если происходит остановка какого-то сегмента сети, то система безопасности должна быть готова к таким событиям.

Клиентское обеспечение систем управления безопасностью, связанное с сервером по этому каналу, должно уметь обрабатывать случаи, когда пропадает связь на каком-либо транзитном участке. При работе в распределенном сетевом окружении всегда надо учитывать потенциальную вероятность отказов по оборудованию и принимать меры к минимизации их влияния на бизнес-процессы.

Для подобных ситуаций существует серьезная методологическая база в рамках Bussiness Continuity и Disaster Recovery процедур. Специалисты нашей компании имеют навыки разработки планов и процедур по данным методологиям и опыт внедрения этих практик.

Переходные ситуации

Надежность системы подразумевает, помимо всего прочего, готовность системы безопасности к возможной переходной ситуации, когда изменения в инфраструктуре произведены еще не полностью. При этом функционирование организации и безопасность информационной инфраструктуры должны обеспечиваться беспрерывно, вне зависимости от того, закончены работы или нет.

Отказ в обслуживании

Когда мы говорим о надежности и доступности, мы также должны учитывать возможные ситуации, когда система безопасности не может по каким-то причинам выполнить поставленные перед ней задачи. Как минимум, система должна их четко детектировать, а сами транзакции или действия осуществлять либо позже, либо обоснованно отвергать их выполнение, поскольку на текущий момент система к этому не готова.

Хорошим примером может служить функционирование почтового шлюза на момент недоступности внутреннего почтового сервера — приходящая почта накапливается до момента возвращения сервера в строй, а если ресурсы шлюза исчерпываются раньше, то клиентам выдается ошибка протокола, вынуждающая послать сообщения позже. Подобное поведение можно рассматривать как правильное в данных условиях.

Ограниченные ресурсы

Немаловажное требование: обслуживание систем должно выполняться ограниченными ресурсами по времени и численности персонала. Хорошие специалисты дорого стоят, и не всякая компания способна держать штат всех необходимых

специалистов нужного уровня. Хорошо спланированная и реализованная, подкрепленная документацией система не требует для эксплуатации большого количества сотрудников, но предъявляет высокие требования к качеству обслуживания.

Свойства системы управления средствами ITSEC в больших системах

Исходя из всего выше сказанного и основываясь на опыте компании «Инфосистемы Джет», сформулируем некоторые свойства «идеальной» системы управления информационной безопасностью в больших и распределенных сетях. К возможным свойствам относятся:

- децентрализованность системы управления безопасностью;
- внимание к планированию, документированию и методологическому обоснованию сопровождения системы;
- способность функционировать в сложных сетевых условиях;
- интеграция системы управления безопасностью с криптографическими средствами;
- оперативная и стратегическая гибкость, открытость системы.

Децентрализованность системы управления безопасностью

Из-за проблем со связью центр управления системой может выйти из строя. В повседневной деятельности необходимо иметь это в виду и обеспечить возможность переключения задач между узлами: скажем, введение резервных центров управления, работы в автономном режиме. Наличие единой точки отказа может дорого обойтись из-за высокой зависимости бизнес-процесса от сетевой инфраструктуры.

Внимание к планированию, документированию и методологическому обоснованию сопровождения системы

Выше уже неоднократно отмечалась необходимость ведения процесса развития информационной системы как регулярной спланированной работы. Важность документирования системы, а также декларирования принципов организации деятельности по ее развитию трудно переоценить.

Актуальность информации о текущем состоянии инфраструктуры, единое мнение о стратегии развития, разработанные и обеспеченные ресурсами планы по реагированию на нештатные ситуации являются ключевыми условиями надежного функционирования информационной системы в будущем.

Способность функционировать в сложных сетевых условиях

Сложностью сетевой инфраструктуры определяется невозможность в большинстве случаев гарантировать ее качество или серьезным образом повлиять на ее состояние. Необходимо добиться, чтобы система управления средствами ITSEC могла «уметь» работать в таких ситуациях. Она должна преодолевать проблемы, связанные с NAT, не зависеть от «шумных» каналов связи с большим количеством ошибок, быть способной пробиваться через слабые каналы связи или хотя бы иметь возможность работать в пограничном режиме.

В общем, несмотря на перечисленные трудности, система управления средствами защиты в больших сетях должна гарантированно и постоянно удерживать контроль над ситуацией.

Интеграция системы управления безопасностью с криптографическими средствами

На текущий момент использование криптографических средств является практичным методом обеспечения необходимых качеств информационной системы — доступности, целостности и конфиденциальности данных и сервисов. Эти технологии позволяют минимизировать ряд серьезных рисков в работе с данными, и пренебрегать ими не стоит.

Оперативная и стратегическая гибкость, открытость системы

Учитывая скорость развития технологий, динамику количественного и качественного усложнения информационных систем, можно предположить, что требования к гибкости и масштабируемости ее элементов будут расти. В динамичной распределенной системе со сложной организационной структурой гибкость и способность к адаптации являются одними из основных свойств.

Заключение

Скорость изменений в современной экономике очень велика, что во многом обеспечивается развитыми средствами связи и технологиями управления информационными ресурсами. Объем и качество данных в определенной мере обуславливают изменения не только в технологии, но и в процессах управления информационными ресурсами. Ценность информационных ресурсов крайне высока, информационные объекты могут обладать значительной самостоятельной стоимостью. Доступность, целостность и конфиденциальность данных, необходимых для обеспечения бизнес-процессов, являются целями построения любой информационной системы. Динамизм и глобальность, потребность в постоянных изменениях резко повышают требования к персоналу и процессам управления в организации, в том числе и к системам обработки информации.

Информационные системы предоставляют возможности для интеграции и взаимодействия различных субъектов в едином информационном пространстве, приводя при этом к невозможности централизованно управлять подобными системами в целом. Все субъекты, совместно использующие информационную систему, как правило, предъявляют к ней разные требования, что ведет к необходимости оперативно и эффективно обеспечивать высокую степень гибкости. Взаимозависимость разных компонентов информационных систем значительно осложняет сопровождение — в большой и сложной системе всегда есть проблемные места, мешающие нормальной работе.

Рассмотренные выше проблемы — это проблемы реальной жизни, известные из опыта внедрения и сопровождения реальных систем. Поскольку это не только технические, но в большой мере организационные проблемы, то полностью решить их только техническими средствами невозможно. В таких ситуациях определяющее значение имеет профессионализм специалистов, обеспечивающих процесс внесения изменений в информационную систему. Обобщение опыта, постоянный планируемый процесс обучения специалистов, создание коллектива высококлассных экспертов по разным вопросам являются очень важными задачами, и в компании «Инфосистемы Джет» им уделяется огромное внимание.

Не менее важно также построение полного цикла обслуживания информационных ресурсов — от консультирования до внедрения и сопровождения, обеспечение организационной составляющей этих процессов, регламентирования взаимодействия между субъектами.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555