Ключевые задачи защиты информации на промышленных предприятиях

При формировании стратегических и тактических планов промышленного предприятия руководство всегда стремится улучшить свои финансовые показатели и обеспечить финансовую устойчивость даже в условиях кризиса. Отношение к роли отдела информационной безопасности компании в этом процессе претерпевает постепенную трансформацию. Если пару лет назад к мерам по обеспечению информационной безопасности у нас в стране относились как к статье затрат, то сейчас зрелые предприятия начинают воспринимать отдел информационной безопасности как бизнес-единицу, обеспечивающую достижение стратегических целей компании. Конечно, только при достаточном уровне зрелости организации можно рассчитывать на определенные дивиденды от усилий, вложенных в построение системы информационной безопасности.

С учетом данной трансформации можно выделить ряд основных задач, которые стоят перед подразделениями ИБ: анализ внешних и внутренних требований и ожиданий заинтересованных сторон (для своевременной оценки рисков и их обработки); определение стратегии обеспечения ИБ, приведенной в соответствие со стратегическими целями бизнеса; определение программы управления ИБ; создание архитектуры и методологической основы комплексной системы безопасности на основе оценки рисков; построение, внедрение и обеспечение повторяемости процессов управления и обеспечения ИБ; контроль и анализ внедренных процессов, работа с событиями и инцидентами ИБ; совершенствование и оптимизация процессов ИБ для наиболее эффективного удовлетворения требований бизнеса.

Эти задачи характерны для организаций любой отрасли. Спецификой промышленных предприятий является то, что самым ценным активом организации является производственный процесс, которому требуется обеспечить непрерывность, в связи с чем сервисы информационной безопасности выступают критичным механизмом для достижения бизнес-целей компании. Этот факт не всегда принимается во внимание, для большинства организаций основным катализатором действий являются внешние регуляторные требования.

ИБ как участник бизнеса

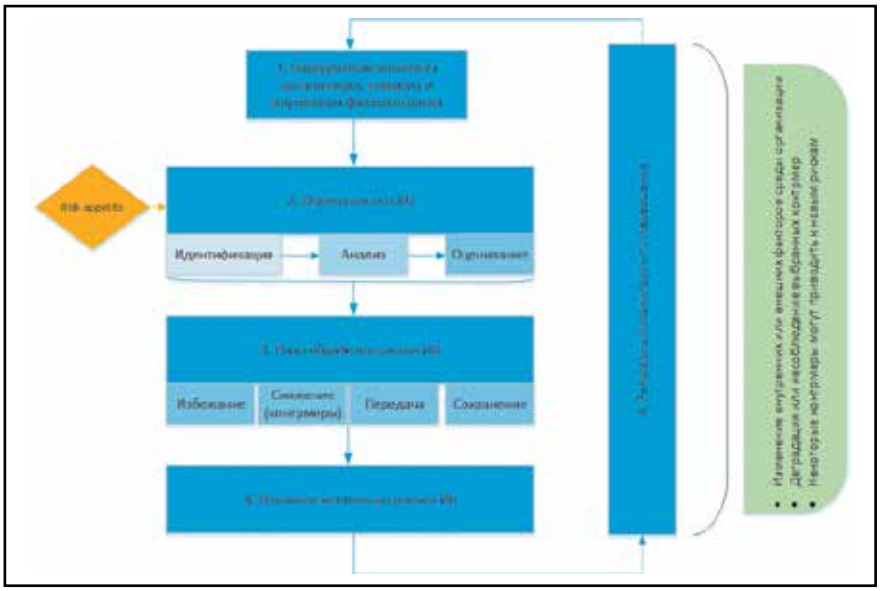
При формировании стратегии и программы управления информационной безопасностью на предприятии краеугольным камнем, независимо от специфики организации, является вовлеченность руководства в данный процесс. Без соответствующей культуры и элементарных навыков у сотрудников в области ИБ, прививаемых "сверху", все усилия окажутся неэффективными и не смогут привести к требуемым результатам.

Привести цели и задачи ИБ в соответствие с целями бизнеса – сложная задача для любой компании. На промышленных предприятиях в условиях критичных производственных процессов просчеты на этом направлении могут стать причиной неправильно сформированных процессов ИБ и вызвать неудовлетворенность как специалистов по безопасности, так и сотрудников производственного блока. В российских условиях компании, как правило, не являются достаточно зрелыми для самостоятельного построения подобных процессов, по крайней мере на начальных этапах. Поэтому они привлекают независимых специалистов либо заключают договоры со специализированными компаниями, что позволяет обеспечить экспертный "взгляд со стороны".

Готовность к переменам

При построении системы обеспечения информационной безопасности в любой компании требования по ИБ должны учитываться еще на этапе разработки информационной системы. Обладая собственным штатом разработчиков, компания может постепенно внедрять процессы SDLC (Security Development Life Cycle), что позволит своевременно обрабатывать риски ИБ. Чем раньше будут вовлечены специалисты по безопасности, тем качественнее будут отработаны требования, которые бизнес предъявляет к системе безопасности на всех уровнях: архитектуры, используемых технологий, бизнес-потоков и т.п.

Необходимо учитывать также то, что практически все корпоративные ИТ-системы в разной степени подвержены изменениям и доработкам – как в архитектуре и взаимосвязях с внешними системами, так и непосредственно в программном коде. Примеры "статичных" ИТ-инфраструктур – редкость. Для компании является критичным определение и достижение соглашения по условиям, которые вызывают необходимость переоценки рисков ИБ. В общем случае это необходимо при изменении факторов внешней и внутренней среды организации.



Управление рисками ИБ в организации

К первым относится, например, появление новых контрагентов, изменение законодательных требований, отраслевых требований и т.д., ко вторым – изменение технологической основы реализации информационных систем, подключение новых АРМ, изменение сетевой структуры.

Моделируя угрозы и оценивая риски ИБ для промышленных предприятий, в частности в сфере производственных процессов, следует понимать, что основной характеристикой, требуемой со стороны бизнеса, будет доступность и целостность информации, конфиденциальность здесь, скорее, уходит на второй план либо не рассматривается – в зависимости от специфики процесса и компании. Важное замечание, о котором часто забывают не только специалисты со стороны заказчика, но и лица, оказывающие услуги: несмотря на используемые методы оценки рисков – количественные, качественные или гибридные, основанные на стандартах NIST, ISO, Octave и т.п. – подход к оценке рисков должен учитывать условия ведения деятельности и культуру отдельно взятой организации. Сложность не всегда означает достижение наилучших показателей. Ведь в конечном счете не стоит забывать, что оценка рисков не ставит своей целью оценку как таковую, а направлена на обеспечение безопасности информационных активов компании и достижение ею стратегических бизнес-целей.

ИБ промышленного холдинга

Сегодня большинство предприятий, в том числе промышленных, объединены в группы, поэтому вопросы управления ИБ должны учитывать как специфику отдельно взятой компании, так и требования всего холдинга. При создании единого интегрированного пространства холдинга важно спланировать структуру процессов управления ИБ на первоначальном этапе и достичь соглашения между всеми участниками процесса.

Как правило, различают три типовые модели управления:

- ***строгую централизацию управления*** на уровне головной организации;
- ***гибридную модель*** с сохранением некоторых управленческих функций на местах и функциями руководства на уровне центра;
- ***децентрализованную модель*** с делегированием всех управленческих функций на уровень отдельных организаций.

Теоретически наиболее правильной представляется модель со строгой централизацией. Она позволяет с наименьшим сопротивлением сформировать единую стратегию и программу ИБ для всей группы компаний, включая подчиненные предприятия. К сожалению, на практике эта модель не всегда оптимальна и подходит далеко не всем заказчикам. Выбор в пользу какой-либо модели нужно сделать, учитывая сложившуюся культуру управления холдингом, готовность к изменениям ИТ-инфраструктуры и процессов управления ИТ, наличие и квалификацию команды ИБ и многие другие факторы.

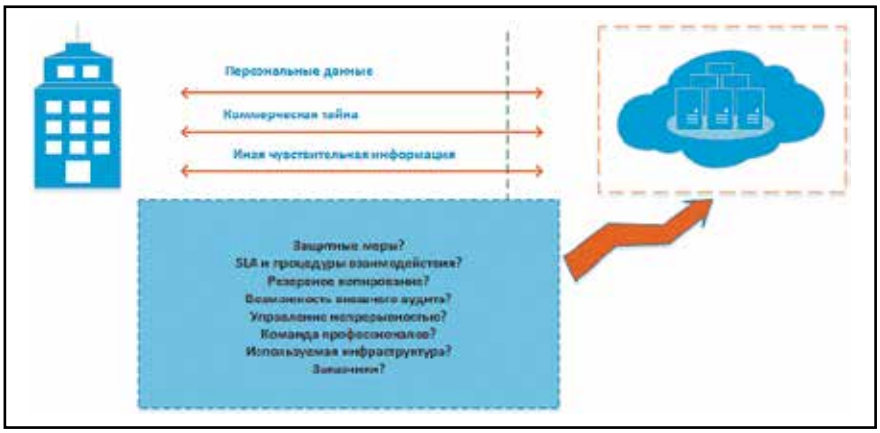
Первым шагом к формированию любой архитектуры управления является изучение контекста организации, аудит ее процессов и информационной инфраструктуры. После этого сравниваются возможные модели управления ИБ на основе соотношения стоимость/эффективность с учетом готовности элементов организации к внедрению соответствующих схем. Выбранная модель определяет построение всех процессов руководства и управления ИБ на уровне холдинга.

Облака – угроза или возможность?

На сегодняшний день многие компании, в большинстве своем иностранные, используют облачные технологии или собираются переводить свою инфраструктуру, отдельные сервисы или информационные системы в облако. Этот путь им представляется наиболее эффективным с точки зрения затрат и получаемых выгод.

Однако вопросы безопасности данных наиболее часто препятствуют использованию облачных сервисов как возможной платформы для ведения бизнеса. Для управления идентифицированными рисками пользователи могут выбирать облачных провайдеров с достаточным для них уровнем SLA, в том числе с описанными в нем механизмами безопасности. Другой возможный вариант – поставить перед выбранными провайдерами задачу обеспечить уровень ИБ, определенный компанией для своих информационных активов.

Любые подобные действия будут упираться в доверие к облачному провайдеру. При выборе поставщика услуг следует удостовериться в возможности аудита и верификации контролей безопасности, используемых облачным провайдером. Компании, которая планирует использовать облачные ресурсы, стоит определить критерии оценки механизмов и процессов провайдера. В качестве базы



Размещение чувствительной информации в облаке. Основные вопросы

могут быть взяты рекомендации следующих стандартов и законодательных актов: AICPA SOC 2, ISO 27001, PCI DSS, ФЗ-152 и т.д.

Необходимо также учитывать финансовое состояние поставщика облачных услуг, наличие сертификации от независимой организации, аттестованных сегментов, реализованных процедур управления непрерывностью бизнеса (в частности, BCP/DRP-планов) и надежных процедур резервного копирования с необходимым уровнем RPO. Важную роль играет квалификация команды поставщика услуг, используемые инфраструктура и приложения, наличие установленных и грамотно сформулированных SLA, матриц взаимодействия, ролевых структур, описаний процессов коммуникации и т.д.

В зависимости от вида облака международная организация ISACA рекомендует обратить внимание на следующие вопросы при переходе или при рассмотрении такой возможности. Если речь идет о модели IaaS (Infrastructure-as-a-Service), нужно предусмотреть варианты снижения воздействия на бизнес организации случаев нарушения (прерывания) предоставления сервиса. При выборе модели PaaS (Platform-as-a-Service) необходимо рассмотреть вопросы доступности, конфиденциальности данных, юридической ответственности и возможности расследования (e-discovery) в случае наступления инцидента ИБ (например, утечки персональных данных). В случае с SaaS (Software-as-a-Service) рекомендуется рассмотреть вопросы права собственности на приложения, места размещения приложений.

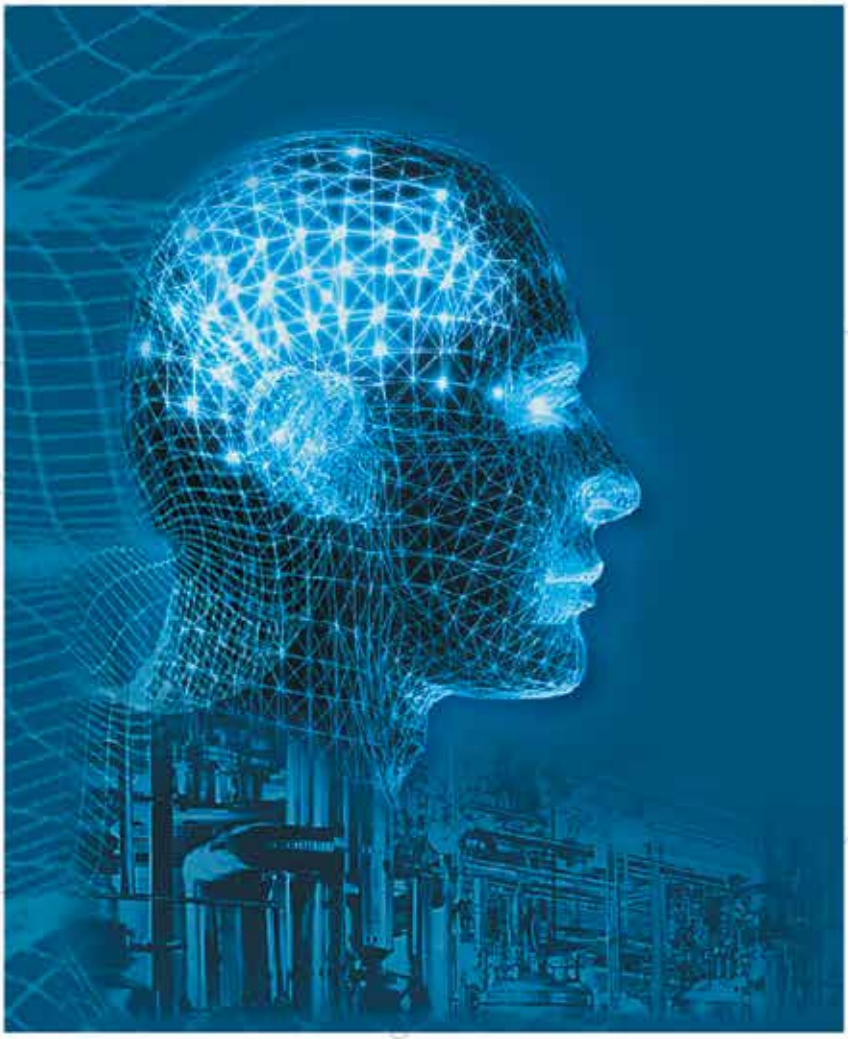
При этом в любом случае, для того чтобы снизить возможные риски, рекомендуется выбирать тех провайдеров, которые обеспечили себе хорошую репутацию на рынке и могут предоставить достаточное количество референсов от своих клиентов.

Алина Хегай, руководитель отдела информационной безопасности, компания "ЛАНИТ-Интеграция" (группа компаний ЛАНИТ)

В РАМКАХ МЕЖДУНАРОДНОГО ПРОМЫШЛЕННОГО ФОРУМА
«РАДИОЭЛЕКТРОНИКА. ПРИБОРОСТРОЕНИЕ. АВТОМАТИЗАЦИЯ»

АВТОМАТИЗАЦИЯ

XVII МЕЖДУНАРОДНАЯ СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА



- **ИКТ в промышленности • Системная интеграция**
- **Автоматизация производства • АСУ ТП**
- **Технические и программные средства автоматизации**
- **Измерение, контроль, испытание, диагностика**
- **Встраиваемые системы • Техническое зрение**
- **Мехатроника и робототехника**
- **Автоматизация зданий и ЖКХ**
- **САПР • Готовые отраслевые решения**

Организатор выставки:

FarEXPO IFE

ais@farexpo.ru, www.farexpo.ru/ais
тел.: +7 (812) 777-04-07, 718-35-37

Место проведения: Санкт-Петербург, СКК, пр. Ю. Гагарина, 8, м. «Парк Победы»

19-21 октября 2016
Санкт-Петербург, Петербургский СКК