Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 3 (178)/2008

Консалтинг в области информационной безопасности

КОРПОРАТИВНЫЕ СИСТЕМЫ

Консалтинг в области информационной безопасности

Олег Слепов, менеджер по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет»

СОДЕРЖАНИЕ НОМЕРА

Сегодня консалтинг является важнейшей составной частью практически любого проекта. Именно поэтому возникла необходимость осветить тему наиболее подробно.

Работая на рынке Информационной безопасности с 1994 года, компания «Инфосистемы Джет» накопила огромный опыт в данной области. Начиная с 2002 года серьезным направлением деятельности становится Консалтинг в области Информационной безопасности.

Что такое консалтинг в области ИБ?

Определение консалтинга в области ИБ

Консалтинг — это, прежде всего, вид интеллектуальной деятельности. Его основная задача заключается в анализе и обосновании перспектив развития, а также в использовании научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента. Консалтинг решает вопросы управленческой, экономической, финансовой, инвестиционной деятельности организаций, стратегического планирования, оптимизации общего функционирования компании, ведения бизнеса, исследования и прогнозирования рынков сбыта, движения цен и т. д. Исходя из вышесказанного, постараемся сформулировать определение консалтинга в области информационной безопасности (далее ИБ).

Консалтинг в области информационной безопасности представляет собой комплекс услуг, оказываемых компанией-консультантом заказчику с целью определения:

- текущего уровня обеспечения (уровня зрелости) ИБ в организации, в соответствии с лучшими мировыми практиками по обеспечению ИБ, отраслевыми требованиями, а также с точки зрения эффективности противодействия существующим угрозам ИБ;
- направления развития ИБ, целей и решаемых задач с учетом стратегических целей развития организации;
- конкретных действий, необходимых для продвижения по выбранному направлению и достижения поставленных целей и задач.

Актуальность услуг по консалтингу в области ИБ

Сегодня консалтинг в области ИБ очень востребован на рынке. Это связано с актуальностью задач, решаемых с его помощью.

В каких же случаях и кто обращается в консалтинговую компанию? Можно выделить четыре основных повода.

Во-первых, это происходит тогда, когда организация не знает, на каком уровне развития находится информационная безопасность ее ресурсов, отвечает ли она потребностям бизнеса и внешним требованиям (законодательство, отраслевые, регулирующие требования, требования заказчиков и т.п.), нет полного понимания, какие действия необходимо предпринимать и нужны ли они вообще. При этом в штате организации отсутствуют квалифицированные специалисты, способные решить вышеперечисленные задачи.

Во-вторых, когда существующая система ИБ построена и функционирует неэффективно, и это сказывается на текущей деятельности. В такой организации часто возникают инциденты информационной безопасности, приводящие к значительным ущербам, остаются высокие риски реализации угроз ИБ из-за отсутствия или малой результативности отдельных мер по ее обеспечению. При этом в организации не хватает необходимого опыта и внутренних ресурсов для выстраивания эффективных защитных мер, а также обеспечения адекватной и своевременной реакции на возникающие инциденты ИБ.

В-третьих, когда существует явная необходимость привести имеющиеся механизмы обеспечения ИБ в соответствие с внешними требованиями в области информационной безопасности. В основном это относится к требованиям различных регуляторов в той отрасли, в которой работает организация. Сюда же можно отнести и выполнение требований законодательства.

В-четвертых, когда организация, достигнув нового, более высокого уровня развития, понимает, что существующий уровень обеспечения ИБ не только не удовлетворяет текущим потребностям, но и является сдерживающим фактором для дальнейшего развития. В данном случае необходимо выстроить процессы управления ИБ, тесно взаимоувязанные с существующими бизнес-процессами, что позволит перевести на более высокую ступень развития и управления ИБ в организации. Это, в свою очередь, поможет добиться прозрачности и ясности вопросов обеспечения информационной безопасности как для высшего руководства организации и существующих акционеров, так и для потенциальных инвесторов. Такой консалтинг заключается в построении системы управления ИБ в соответствии с лучшими мировыми практиками и, при необходимости, в подготовке системы управления к сертификации[1] по международным стандартам в области ИБ.

Инициаторами приобретения услуг консалтинга в сфере информационной безопасности, как правило, являются:

- **руководство организации**, если оно хочет разобраться в том, на каком уровне находится ИБ в организации, сделать ее эффективной с точки зрения затрат и, соответственно, адекватной угрозам, что необходимо предпринять, чтобы улучшить состояние процессов обеспечения защиты информации. При этом руководство осознает, что собственных ресурсов для решения такой задачи недостаточно. В некоторых случаях руководство может быть инициатором приглашения внешнего консультанта, если хочет составить для себя объективную картину того, насколько качественно службы, ответственные за выполнение задач по обеспечению ИБ, выполняют их;
- **служба автоматизации или служба информационной безопасности**, когда существующий уровень компетенций сотрудников в части ИБ в целом недостаточен для решения поставленных задач по построению эффективной системы информационной безопасности;
- **служба информационной безопасности** в случаях, когда перед ней ставятся новые задачи, выходящие за рамки установленных обязанностей и компетенций (периодические работы, требующие высокой квалификации со-

1 Вопросы сертификации в большинстве случаев связаны с планируемым привлечением инвестиций, с выходом организации на IPO, с упрочнением позиции на рынке, созданием необходимого имиджа в глазах потенциальных партнеров и повышением доверия со стороны клиентов.

трудников, внедрение новых систем и технологий и т.п.). В данном случае внешние высококвалифицированные специалисты привлекаются для решения данных специализированных задач, в то время как штатные сотрудники службы могут сконцентрироваться на решении профильных повседневных вопросов.

Виды консалтинга в области информационной безопасности

Каждый консалтинговый проект в области ИБ сам по себе уникален. Однако можно выделить основные виды услуг, предоставляемых консалтинговыми компаниями:

- аналитическая деятельность (анализ и оценка деятельности организации по защите информационных ресурсов, включая анализ эффективности применяемых средств и методов защиты информации, экспертизу ведущихся проектов в части ИБ, сравнительные исследования с показателями по отрасли и т. д.);
- прогнозирование (на основе проведенного анализа и используемых консультантом методик — составление прогнозов по указанным выше направлениям);
- консультации с выдачей рекомендаций по самому широкому кругу вопросов, касающихся защиты бизнес-процессов и ресурсов организации, разработки и внедрения мероприятий и систем защиты;
- стратегическое планирование деятельности организации в области ИБ и решение совокупности проблем, связанных с организацией управления информационной безопасностью.

Формы оказания услуг по консалтингу в области информационной безопасности

Формы предоставления услуг также могут быть различными в зависимоси от сложности проекта и пожеланий заказчика:

- консультации с периодическими выездами на площадку заказчика для сбора исходных данных, согласования результатов анализа и выдаваемых рекомендаций;
- удаленные консультации без выезда на площадку заказчика;
- постоянное присутствие на площадке заказчика определенного числа консультанов в течении всего срока проекта (аутстаффинг).

Определение уровня информационной безопасности

Для определения уровня информационной безопасности, который обеспечивается в организации, проводится обследование состояния ИБ организации. Однако само по себе обследование не имеет смысла, если в результате не будут выработаны рекомендации по повышению уровня защищенности от существующих угроз в отношении информационных ресурсов компании.

Чаще всего такие работы называются аудитом информационной безопасности. Однако, по мнению экспертов компании «Инфосистемы Джет», понятия аудит и обследование стоит различать. Аудиты проводятся, как правило, с целью сбора доказательств соответствия определенному стандарту или нормативному акту деятельности организации в области обеспечения ИБ. И результатом аудита обычно является аудиторский отчет с указанием выявленных несоответствий, не содержащий конкретных рекомендаций по их устранению.

Обследование же, являясь по сути консультациями сотрудников заказчика, позволяет провести более глубокое изучение состояния информационной безопасности. Его целью является не столько поиск несоответствий и свидетельств наличия этих несоответствий, сколько определение причин существующих проблем и выработка необходимых эффективных действий и мероприятий, которые помогут в их решении и приведут имеющиеся механизмы обеспечения ИБ в соответствие с требованиями по информационной безопасности, предъявляемыми к организации.

Обследование состояния ИБ — это наиболее востребованная, а потому и самая распространенная услуга по консалтингу в области информационной безопасности.

Обследование состояния информационной безопасности с разработкой рекомендаций

Данная услуга заключается, главным образом, в оценке текущего уровня защищенности информационных систем (далее ИС) организации. На основе полученных сведений, разрабатываются рекомендации по реализации комплекса организационных и технических мер, повышающих существующий уровень ИБ.

Такое обследование, как правило, проводится на начальном этапе работ по созданию комплексной системы информационной безопасности компании.

В число задач, решаемых при проведении работ по обследованию состояния информационной безопасности заказчика, входит:

- оценка состояния системы ИБ организации;
- оценка соответствия механизмов системы информационной безопасности организации выбранным критериям обследования;
- выявление актуальных проблем, связанных с обеспечением ИБ;
- формирование оптимальной и эффективной программы построения системы информационной безопасности организации.

В зависимости от задач, стоящих перед организацией, обследование состояния ИБ может включать в себя различные виды работ и критерии оценки, которые согласуются с исполнителем перед началом консалтингового проекта. В целом, все работы в ходе обследования выполняются в 3 этапа:

- информационное обследование;
- анализ полученной в ходе обследования информации;
- разработка и согласование рекомендаций по повышению уровня информационной безопасности организации.

Информационное обследование

Информационное обследование проводится с целью сбора и обработки всех данных, необходимых для принятия решения по определению текущего уровня защищенности ИС компании и разработке рекомендаций по его повышению. Такое обследование включает в себя сбор сведений:

- об информационной системе организации, защищенность которой будет оцениваться в ходе работ;
- о процессах обеспечения информационной безопасности в организации;
- о текущем уровне защищенности ИС.

Сбор данных об информационной системе организации

Работы этого этапа включают получение сведений:

- об организационной структуре заказчика;
- о структуре комплекса используемых программно-технических средств;
- о характеристиках используемых каналов и точек подключения к сетям связи и сети Интернет;
- о структуре информационных потоков в ИС.

Информационное обследование также может включать сбор информации о следующих системах и сервисах:

- прикладные автоматизированные системы:
  - автоматизированные системы управления деятельностью организации (для промышленных предприятий — АСУТП; для кредитно-финансовых организаций — АБС, процессинговые системы, системы дистанционного банковского обслуживания; для телекоммуникационных компаний — автоматизированные системы расчетов с абонентами и т.п.);
  - системы управленческого анализа;
  - системы класса CRM/ERP;
  - средства подготовки и отправки отчетности;
  - системы электронного документооборота и т.п.;
- инфраструктурные автоматизированные системы и сервисы:
  - службы каталогов;
  - сервисы ЛВС;
  - беспроводные системы и сервисы (WiFi, Bluetooth и т.п.);
  - службы терминального доступа;
  - электронная почта;
  - сервис доступа в сеть Интернет;
  - сервис файлового обмена и т.п.

Сбор информации о процессах обеспечения информационной безопасности

Сбор информации о процессах обеспечения ИБ в организации проводится с целью оценки общего состояния данных процессов и их соответствия целям компании. При этом консультанты знакомятся с организационно-распорядительными документами по ИБ, утвержденными в обследуемой организации, а также проводят интервью с представителями высшего руководства, с руководителями основных и вспомогательных подразделений заказчика.

В процессе выполнения работ на данном этапе проводится:

- оценка зрелости процессов ИБ;
- оценка степени внедрения процессов информационной безопасности с целью выяснения того, насколько широко применяются рассматриваемые процессы;
- анализ существующей нормативно-распорядительной документации по обеспечению ИБ.

При анализе нормативно-распорядительной документации проводится проверка наличия в организации нормативно-регламентирующей базы по обеспечению информационной безопасности:

- организационной инфраструктуры с установленными обязанностями по обеспечению информационной безопасности для сотрудников всех должностей;
- утвержденной политики обеспечения информационной безопасности (политика парольной защиты, политика антивирусной защиты, политика реагирования на нарушения ИБ, политика использования ресурсов сети Интернет, положение о конфиденциальности и т.п.);
- документированных правил обращения с информационными ресурсами, включая правила отнесения данных к определенным категориям (перечень сведений, составляющих конфиденциальную информацию, регламент назначения и разграничения прав доступа к данным);
- документированных процессов обслуживания и администрирования информационной системы и используемых средств защиты, а также мер обеспечения бесперебойной работы.

Кроме того, в ходе работ специалистами компании-консультанта проводится экспресс-опрос сотрудников бизнес-подразделений организации с целью определения уровня знания, понимания и соблюдения положений политики и других документов по ИБ.

Результатом работ на данном этапе является оценка зрелости существующих процессов информационной безопасности и полноты существующих нормативно-регламентирующих документов, а также их применения сотрудниками в своей повседневной деятельности.

Сбор информации о защищенности информационной системы

На рассматриваемом этапе собираются данные о встроенных механизмах обеспечения информационной безопасности в прикладных и инфраструктурных системах, а также об используемых наложенных средствах защиты информации.

Этап сбора информации о текущем уровне защищенности ИС может также включать инструментальный анализ защищенности информационной системы организации[2], который делится на две части: анализ защищенности внешних и внутренних ресурсов ИС.

Инструментальный анализ из сети Интернет имитирует действия внешних злоумышленников, которые обладают высоким уровнем знаний в области вычислительной техники и получают информацию об ИС из открытых источников.

Результатом таких работ является экспертная оценка потенциальной возможности совершения несанкционированного воздействия или нанесения ущерба ресурсам информационной системы со стороны внешних злоумышленников.

Внутренний инструментальный анализ имитирует действия внутренних злоумышленников, являющихся зарегистрированными пользователями информационной системы организации.

Результатом этих работ является экспертная оценка потенциальной возможности совершения несанкционированного воздействия или нанесения ущерба ресурсам информационной системы со стороны внутренних злоумышленников, а также защищенности эксплуатируемых в информационной системе прикладных систем, операционных систем и баз данных.

Анализ полученной информации

На этом этапе проводится экспертная оценка текущих показателей защищенности основных ресурсов ИС, определяется возможность нарушения конфиденциальности, целостности и доступности ресурсов информационной системы с использованием выявленных уязвимостей внешними и внутренними нарушителями.

Критериями принятия решений при анализе полученной информации и выработке рекомендаций являются:

- экспертное мнение специалистов компании-консультанта, имеющих большой опыт предоставления консалтинговых услуг организациям различных областей деятельности;
- мнение высшего руководства организации;
- результаты интервью с персоналом организации;
- требования законодательства;
- требования нормативных документов и стандартов как отраслевых, так и самой организации.

Результатом работ на данном этапе является экспертная оценка эффективности используемых средств и методов защиты информационных ресурсов ИС. Кроме того, с учетом результатов предыдущих этапов, строится модель угроз информационной безопасности в отношении ресурсов ИС организации.

2 Необходимо отметить, что инструментальный анализ защищенности, по мнению специалистов компании «Инфосистемы Джет», должен проводиться после модернизации системы обеспечения информационной безопасности заказчика с целью проверки эффективности внедренных мер по повышению уровня защищенности ИС.

Предложение компании «Инфосистемы Джет»: «Обследование состояния ИБ с разработкой рекомендаций по повышению уровня защищенности организации»

При обследовании состояния ИБ компания «Инфосистемы Джет» использует экспертный подход. Он заключается в учете экспертного мнения специалистов компании «Инфосистемы Джет», имеющих богатый опыт проведения консалтинговых работ в организациях различных вертикальных рынков.

Для повышения эффективности работ и предоставления заказчику наиболее достоверных результатов консультанты компании «Инфосистемы Джет» предъявляют жесткие требования к методике проведения обследования состояния информационной безопасности. К ним относятся:

1. **Объективность (достоверность) результата обследования состояния ИБ.** Консультанты компании «Инфосистемы Джет» предоставляют заказчику обоснование наличия угроз информационной безопасности и уязвимостей, которые существуют в информационной системе организации, а также возможных последствий (ущерба) в случае их реализации.
2. **Глубина обследования состояния ИБ.** В ходе обследования специалисты компании «Инфосистемы Джет» (с учетом интересов заказчика) выбирают для проверки наиболее критичные области деятельности и процессы организации, что позволяет получить более детальные данные для анализа.
3. **Критерии оценки защищенности, согласованные с заказчиком.** Понятные критерии оценки защищенности — одно из важных условий корректного восприятия результатов обследования. К таким критериям относятся:
   - требования законодательства Российской Федерации в области ИБ;
   - отраслевые требования по обеспечению ИБ;
   - бизнес-требования обследуемой организации;
   - нормативно-методические и организационно-распорядительные документы и стандарты в области ИБ, существующие в организации;
   - контрактные обязательства заказчика (партнерские договоры, контракты с поставщиками и т.п.).

Benchmarking

В своих консалтинговых работах специалисты компании «Инфосистемы Джет» используют и такой аналитический инструмент как benchmarking. В данном случае на русский язык этот термин можно перевести как «метод аналогов». Этот метод иногда рассматривается как «экспресс-анализ рисков», поскольку не требует глубокой оценки рисков ИБ на начальных этапах проведения работ. Собираются лишь статистические сведения, характерные для большинства компаний по отрасли, и на их основе проводится сравнение.

Benchmarking может эффективно использоваться для оптимизации текущей деятельности организации по обеспечению ИБ: оценивая эффективность деятельности организации по сравнению с другими организациями в той же отрасли и анализируя причины этих различий, можно формулировать необходимые шаги для повышения эффективности обеспечения ИБ до уровня «лучших» в отрасли. С другой стороны, применяя «метод аналогов», можно выявить собственную уникальность организации в реализации процессов обеспечения информационной безопасности.

Консультанты компании «Инфосистемы Джет» используют различные виды benchmaring (см. Рис.1), начиная со сравнения эффективности подразделений внутри организации и заканчивая сравнением эффективности функций компаний в целом по отрасли. В последнее время интерес вызывают такие виды, как benchmarking конкурентоспособности, когда идет сравнение эффективности деятельности компании по обеспечению ИБ с конкурентами в той или иной области, или benchmarking затрат, где сравнивается уже бюджеты на ИБ по отрасли.

Построение модели угроз

На данном этапе осуществляется классификация и описание угроз и уязвимостей, обнаруженных в информационной системе заказчика с экспертной оценкой возможных последствий реализации выявленных угроз.

В итоге этих работ является модель угроз, классифицированных по уровню критичности для организации. Такая модель включает описание угрозы, в том числе агента реализации угрозы, выявленных уязвимостей, активов, в отношении которых возможна реализация угрозы, типов воз-

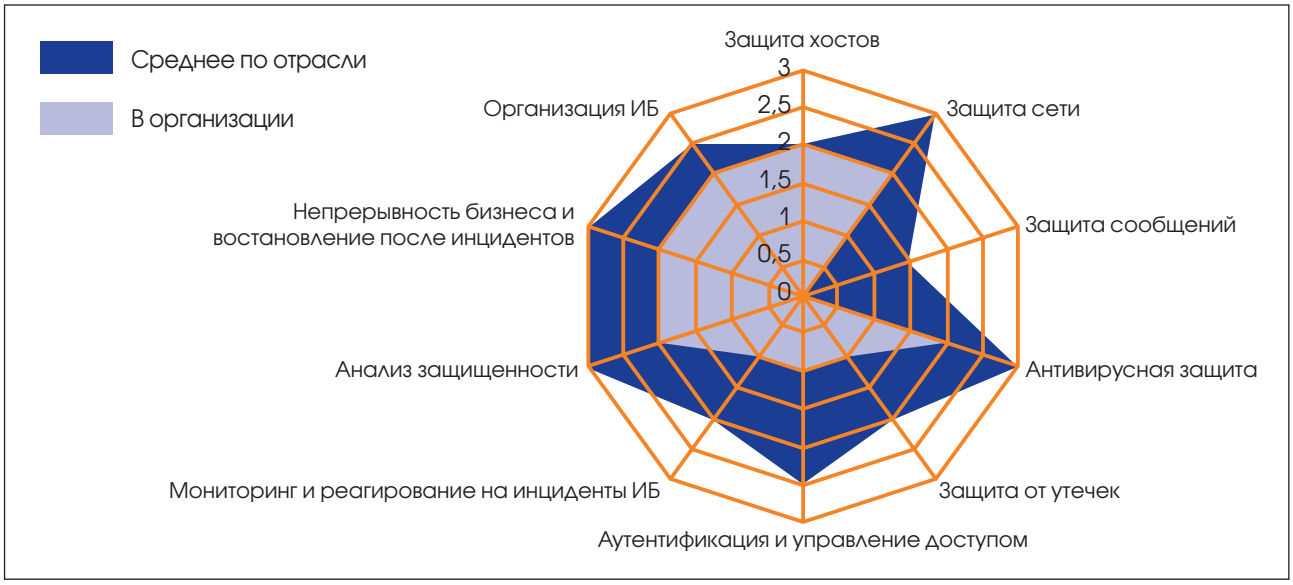


Рис.1. Пример результатов benchmarking: сравнение со средними показателями по отрасли

можных потерь в случае нарушения конфиденциальности, целостности или доступности активов.

Степень детализации модели угроз может быть различна и определяется реальными потребностями для каждой организации в отдельности.

Подготовка рекомендаций

По результатам проведенного обследования подготавливается отчет, который включает в себя описание:

- обследованных автоматизированных систем (далее — АС), сервисов и программно-технических средств;
- существующих административных и организационных мер по обеспечению ИБ;
- применяемых программно-технических средств обеспечения ИБ;
- рекомендаций по применению комплекса мер и средств, которые необходимо реализовать для повышения уровня информационной безопасности компании.

Рекомендации могут включать:

- первоочередные меры по усилению информационной безопасности ИС заказчика (ряд технических и организационных мероприятий, проведение которых должно быть осуществлено незамедлительно);
- изменения или дополнения, которые необходимо внести в нормативно-распорядительную документацию (в том числе в политику обеспечения информационной безопасности), и механизмы доведения ее до пользователей ИС заказчика;
- доработку существующих механизмов защиты данных в ИС (например, изменение конфигураций и настроек внешних и встроенных средств защиты информации, прикладных АС);
- внедрение дополнительных механизмов защиты информации.

Анализ рисков информационной безопасности

Другим подходом, позволяющим наиболее глубоко оценить текущее состояние информационной безопасности и вывести ее на более высокий уровень развития, является анализ рисков ИБ. Как правило, он характерен для компаний с более продвинутой системой менеджмента, где уже сформирован и функционирует отдел, в задачи которого входит оценка операционных рисков. Анализ рисков ИБ рассматривается как бизнес-задача, инициируемая руководством организации в силу своей информированности и степени осознания проблем ИБ, смысл которой заключается в защите бизнеса от реально существующих угроз ИБ.

При анализе рисков ИБ консалтинговые компании обычно знакомятся с организационно-распорядительными документами по информационной безопасности, проводят интервью с представителями высшего руководства заказчика, с руководителями основных направлений деятельности и обеспечивающих подразделений с целью оценки общего состояния процессов обеспечения ИБ и их соответствия бизнес-целям заказчика.

При проведении анализа рисков ИБ рассматриваются следующие основные бизнес-процессы:

- развитие бизнеса;

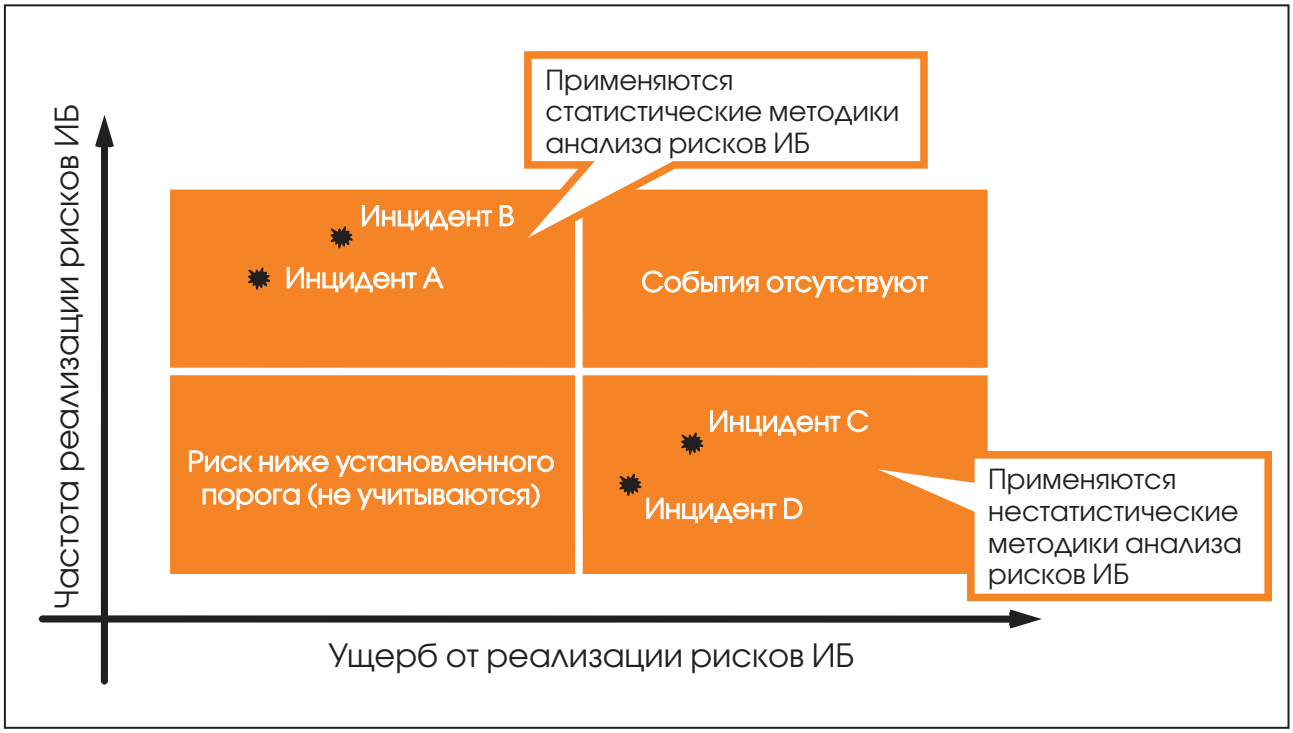


Рис. 2 Практика применения статистических и нестатистических методик анализа рисков ИБ

- планирование и подготовка финансовой отчетности;
- управление персоналом;
- внутренний аудит;
- управление проектами;
- продажи;
- производство или предоставление услуг.

Работы по анализу рисков ИБ включают в себя несколько этапов, описанных ниже.

Идентификация и оценка критичности активов

Процесс анализа рисков ИБ начинается с идентификации и оценки критичности активов организации. Идентифицируются все активы, задействованные в функционировании бизнес-процессов и имеющие влияние на ценную для компании информацию. Данные активы включают:

- человеческие ресурсы;
- информационные ресурсы (как в электронном, так и в бумажном виде);
- оборудование;
- программное обеспечение;
- услуги, оказываемые внутренним и внешним заказчикам.

Оценка критичности (или ценности) каждого актива формулируется владельцем данного актива. Результатом этого этапа является полный перечень активов, их критичности и список владельцев, оформленный в виде отчета по инвентаризации активов.

Разработка методики анализа рисков

Для любой организации характерны свои риски, в том числе и риски информационной безопасности. Именно поэтому при их оценке необходимо учитывать все специфические моменты, связанные с функционированием организации. Такой учет проводится на этапе разработки методики анализа рисков ИБ.

Существуют различные методики анализа рисков ИБ. Условно их можно разделить на статистические и нестатистические методики (Рис.2).

Статистические методики применяются в случае, если в организации накоплена достаточная база событий ИБ, поскольку данный метод основывается как раз на собранных статистических данных об инцидентах, связанных с нарушением информационной безопасности.

Но что делать, если таких событий мало? Тогда используются нестатистические методы, к которым относятся, например, вариационный метод, метод имитационного моделирования, а также наиболее популярная в настоящее время методика анализа сценариев. Она, в частности, применяется для оценки рисков редких событий с большими операционными потерями, а также в случае, если внутренних исторических данных недостаточно для применения статистических методик. Использование методики анализа сценариев является, к примеру, требованием соглашения Basel II при оценке рисков редких событий в кредитно-финансовых организациях.

Предложения компании «Инфосистемы Джет»: «Внедрение процесса управления рисками ИБ»

Специалистами компании «Инфосистемы Джет» разработан комплекс специальных услуг, которые можно озаглавить как «Внедрение процесса управления рисками ИБ».

Первый блок услуг данного комплекса предполагает оценку специалистами компании «Инфосистемы Джет» текущего состояния ИБ в наиболее критичных бизнес-системах заказчика через оценку рисков ключевых бизнес-процессов и связанных с ними информационных систем. В результате вырабатываются рекомендации по внедрению дополнительных и повышению эффективности существующих административных, организационных мер и программно-технических средств и методов защиты информации. Данные рекомендации ложатся в основу плана обработки рисков — детального плана внедрения мер по обеспечению ИБ с оценкой эффективности их реализации.

Для кредитно-финансовых структур компания «Инфосистемы Джет» разработала услугу по оценке рисков ИБ в соответствии с соглашением Basel II. При этом риски ИБ рассматриваются как часть операционных рисков.

Второй блок услуг предполагает построение специалистами компании «Инфосистемы Джет» процесса управления рисками информационной безопасности в организации заказчика. В отличие от оценки рисков ИБ, работы предполагают внедрение необходимых мер и процедур, которые в дальнейшем позволят компании самостоятельно осуществлять оценку рисков. Помимо методики, разработанной с учетом реалий и требований заказчика, и плана обработки рисков организация получает работающий процесс управления рисками. Этот процесс обязательно предполагает наличие обученного персонала, а также специальных регламентов по управлению рисками ИБ в компании.

При создании методики анализа рисков ИБ большое значение имеет разработка процедуры анализа рисков, которая должна учитывать специфику бизнес-процессов заказчика. Она утверждается высшим руководством организации.

На этапе разработки методики анализа рисков ИБ также осуществляется выбор шкалы уровней риска, определение приемлемого уровня риска, а также разработка критериев, на основании которых достигается снижение критичных рисков до приемлемого уровня.

Идентификация рисков

На этапе идентификации рисков информационной безопасности с использованием разработанной процедуры анализа рисков специалистами компании-консультанта проводятся:

- идентификация угроз информационной безопасности в отношении сформированного перечня активов;
- идентификация уязвимостей, которые могут привести к реализации угроз;
- идентификация потенциального ущерба (последствий реализации угроз), к которому может привести нарушение информационной безопасности активов.

Результатом данных работ является документированный набор идентифицированных рисков.

Оценка рисков

Оценка рисков информационной безопасности является важнейшим элементом процесса анализа рисков ИБ и включает в себя целый комплекс мероприятий:

- оценка ущерба для бизнеса, который возможен в результате нарушения информационной безопасности активов;
- оценка возможности нарушения информационной безопасности активов с учетом идентифицированных для данных активов угроз, уязвимостей и ущерба, а также используемых механизмов информационной безопасности;
- определение уровней (величин) рисков.

Выбор мер противодействия рискам

Заключительным этапом процесса анализа рисков ИБ является выбор мер противодействия. Данный этап подразумевает сопоставление определенных уровней рисков с выбранными на предыдущих этапах критериями для их принятия или снижения.

Результатом является комплекс механизмов контроля, направленный на снижение выявленных рисков. Разрабатывается и утверждается высшим руководством организации «План обработки рисков», описывающий решения по их принятию или снижению с указанием выбранных мер и мероприятий. В плане также указываются приоритеты снижения, действия конкретных исполнителей, бюд-

жетируются конкретные мероприятия и средства защиты информации.

Реализация разработанного плана обработки рисков ИБ является основой для бизнес-ориентированного подхода к обеспечению информационной безопасности в организации.

Результаты анализа рисков ИБ

Результатом работ по анализу рисков информационной безопасности, как правило, является:

- описание обследованных автоматизированных систем и сервисов, применяемых административных, организационных мер, программно-технических средств обеспечения ИБ;
- карта рисков информационной безопасности;
- план обработки рисков, который включает комплекс внедряемых административных, организационных мер и программно-технических средств, направленных на снижение уровня рисков информационной безопасности, оценку стоимости внедрения, а также график мероприятий по внедрению мер обеспечения ИБ (а в некоторых случаях полученные данные могут быть представлены в виде эскизного проекта реализации системы информационной безопасности ИС заказчика).

Обеспечение требований бизнеса к информационной безопасности

Цели, задачи и направления развития информационной безопасности должны определяться на основе требований бизнеса в лице руководства, функциональных и вспомогательных подразделений, участвующих в процессе производства. Именно бизнес, являясь основным «владельцем» информационных активов организации, должен определять требования по их защите. Формирование требований происходит путем взаимной увязки целей бизнеса и ИБ. В настоящее время основным способом достижения этого является разработка стратегии информационной безопасности.

Разработка стратегии информационной безопасности

Стратегия ИБ — это единый документ, утвержденный руководством организации, который определяет подходы к обеспечению информационной безопасности на продолжительный срок. Она определяет цели и задачи системы обеспечения ИБ, принципы ее организации, функционирования и управления, а также основные направления создания и развития целостной системы обеспечения безопасности информации заказчика.

Стратегия ИБ включает в себя правовые, оперативные, технологические, организационные, технические и физические меры по защите информации, которые находятся в тесной взаимосвязи между собой.

Стратегия ИБ определяет направления обеспечения ИБ во всех областях деятельности заказчика и на всех участках его информационных и автоматизированных систем. При ее разработке должны учитываться цели и потребности компании, ее организация, структура и размещение информационных и коммуникационных систем, характер решаемых бизнес-задач и перспективы развития информационных технологий.

Она служит методологической основой для составления нормативно-методических и организационно-распорядительных документов, а также внедрения практических мер, методов и средств защиты информации. Стратегия ИБ является долгосрочным документом и пересматривается по решению руководства заказчика в случае кардинальных изменений направления бизнеса организации или внешних условий его ведения.

В число задач, решаемых при ее разработке, входят:

- формирование целостного представления и системы взглядов на обеспечение информационной безопасности заказчика и взаимоувязка различных ее элементов;
- определение путей развития ИБ, основополагающих целей и задач системы обеспечения ИБ;
- определение путей реализации мер, обеспечивающих необходимый уровень надежной защиты информационных ресурсов;
- создание методологической основы для разработки нормативно-методических и организационно-распорядительных документов по ИБ, практических мер, методов и средств защиты информации.

Разработка стратегии ИБ включает в себя несколько этапов.

Первым этапом является сбор и анализ информации, необходимой для разработки стратегии обеспечения ИБ. На данном этапе специалисты компании-консультанта знакомятся с организационно-распорядительными документами по ИБ, ут-

вержденными в организации заказчика, а также проводят интервью с представителями высшего руководства заказчика, с руководителями основных направлений бизнеса и обеспечивающих подразделений с целью:

- определения стратегических бизнес-целей организации;
- идентификации требований руководства, подразделений Информационных технологий и Информационной безопасности по обеспечению ИБ;
- анализа организационной структуры и ролей персонала по обеспечению ИБ;
- оценки соответствия действующих мер безопасности идентифицированным требованиям руководства, подразделений Информационных технологий и Информационной безопасности по обеспечению ИБ;
- идентификации критичных бизнес-процессов организации;
- идентификации ключевых информационных систем и сервисов;
- определения наиболее значительных для организации рисков ИБ.

На этапе сбора основной информации о процессах ИБ проводятся интервью со следующими ответственными лицами:

1. Высшее руководство организации.
2. Руководители, ответственные за:
   - развитие бизнеса;
   - подготовку финансовой отчетности;
   - управление персоналом;
   - управление ИТ;
   - управление ИБ;
   - управление операционными рисками;
   - внутренний аудит.
3. Руководители, ответственные за основные направления бизнеса.
4. Руководители и специалисты, ответственные за основные области ИТ и информационной безопасности.

Второй этап — собственно разработка документа «Стратегия информационной безопасности», который включает в себя следующие разделы[3]:

- введение;
- общие положения;
- цели, задачи и стратегии обеспечения информационной безопасности;
- основные принципы обеспечения информационной безопасности;
- соответствие требованиям[4] нормативно-правовых актов в области ИБ;
- описание программ по основным направлениям развития ИБ, в том числе описание программы по модернизации организационной структуры и ролей персонала по обеспечению ИБ.

Разработка документа осуществляется в контексте:

- целей бизнеса организации;
- ключевых характеристик деятельности организации и ее основных бизнес-процессов;
- территориального распределения инфраструктуры организации;
- действующих законодательных норм и договорных обязательств;
- системы нормативно-распорядительной документации по обеспечению ИБ;
- организационной структуры и ролей персонала по обеспечению ИБ;
- рекомендаций российских и международных стандартов и лучших практик в области ИБ.

Стратегия ИБ включает в себя описание программ по основным направлениям развития ИБ. В качестве примера можно привести такие, как «Внедрение процессов управления ИБ», «Разработка требований ИБ для политики ИБ», «Разработка и внедрение процедур безопасного взаимодействия со сторонними организациями», «Внедрение системы управления доступом и контроля использования ресурсов ИС» и т.п. Перечень и состав данных программ зависит от бизнес-целей и задач организации, которые выявляются в ходе сбора и анализа данных. В свою очередь каждая программа содержит ориентировочный перечень проектов, необходимых для ее реализации, с примерными сроками их реализации.

Также в стратегию ИБ включается описание программы по модернизации организационной структуры и ролей персонала по обеспечению ИБ. Данная программа должна содержать необходимые изменения штатно-организационной и ролевой структуры, ориентировочную оценку требуемых на это ресурсов.

На заключительном этапе разработки стратегия ИБ обязательно согласовывается и утверждается руководством заказчика.

3 Это приблизительный перечень разделов, их количество, наименование и содержание зависит от результатов анализа собранных данных.

4 В данном разделе приводится перечень законодательных требований и стандартов, которым необходимо соответствовать или которыми необходимо руководствоваться организации при реализации стратегии ИБ.

Обеспечение требований законодательства[5]

Как говорилось в начале статьи, актуальность услуг консалтинга в области ИБ в значительной степени связана с необходимостью приведения информационной безопасности в соответствие с требованиями законодательства.

Информационная безопасность — это, пожалуй, одна из тех областей, которая должна быть жестко регламентирована, поскольку применение непроверенных практикой и неформализованных норм чревато серьезными негативными последствиями для владельцев и пользователей информации.

Основным регулятором, контролирующим выполнение требований по обеспечению ИБ, является государство. Оно должно устанавливать отношения, связанные с обменом данных, поскольку, во-первых, взаимоотношения в информационной сфере находятся в области его прямых интересов, во-вторых, оно должно контролировать баланс интересов граждан, общества и государства.

Российское законодательство не отличается жесткостью регулирования отношений в области информационной безопасности. Серьезные требования по защите предъявляются лишь к сведениям, относящимся к государственной тайне. Что касается защиты, например, коммерческой и другой подобной информации, то государство и регулирующие органы отдают это на откуп самим коммерческим организациям, предоставляя им полную свободу выбора как методов, так и средств защиты данных, относящихся к коммерческой тайне.

Другая проблема российского законодательства заключается в том, что законодательные и регулирующие органы просто не успевают за изменениями, происходящими в сфере информационных технологий. Если законы в этой области издаются, то они, как правило, не работают в полном объеме из-за потери актуальности, поскольку принимались слишком долго, а ситуация уже изменилась. Примером может служить закон об электронно-цифровой подписи (далее ЭЦП), который должен был способствовать развитию российской информационной инфраструктуры и услуг, росту продаж в российском сегменте Интернета, ранее сдерживаемом отсутствием надежных процедур аутентификации. Однако этот закон ничем не облегчил применение ЭЦП в корпоративных системах и пока не привел к применению ее в системах общего пользования. Кроме того, требование обязательного использования в системах общего пользования только сертифицированных средств, т. е. отечественных криптоалгоритмов ЭЦП, существенно ограничило рамки этих систем.

Все же необходимо отметить положительные сдвиги в сфере нормативно-правового регулирования в области ИБ в России. Так, серьезные инциденты, связанные с кражами баз данных пользователей информационных систем, происходивших в России на протяжении последних лет, привели к необходимости принятия специальных требований, которые бы жестко регулировали обработку, хранение и передачу персональных данных пользователей. Так в 2006 году был создан закон о персональных данных.

Требования к защите персональных данных

Полное наименование: Федеральный закон Российской Федерации «О персональных данных» №152-ФЗ от 27.07.2006. Он регулирует отношения между организациями, субъектами персональных данных (далее ПДн) и физическими лицами, являющимися операторами информационных систем[6], с помощью которых обрабатываются ПДн. Закон устанавливает область и характер ответственности оператора, обрабатывающего персональные данные, а также определяет контролирующие органы по защите прав субъектов ПДн.

На сегодняшний день государство и регулирующие органы уже начали формировать единый пакет документов, определяющий все аспекты обработки, хранения и передачи персональных данных пользователей информационных систем. Так, внесены изменения в «Трудовой Кодекс Российской Федерации» №197-ФЗ от 30.12.01 г., касающиеся персональных данных. Принято Постановление Правительства Российской Федерации «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказами ФСБ России, ФСТЭК России и МИТС России определен порядок проведения классифи-

5 Целью данной статьи не является обзор практики нормативно-правового регулирования в сфере защиты информации. Автор ставит задачу рассказать о наиболее актуальных на данный момент законодательных и нормативно-правовых актах и услугах, связанных с приведением информационной безопасности в соответствие с их требованиями.

6 Персональные данные могут обрабатываться как с помощью средств автоматизации, так и без них. В последнем случае рассматриваются информационные системы, которые по характеру действий, совершаемых с персональными данными, схожи с системами, в которых используются средства автоматизации.

Предложение Компании «Инфосистемы Джет» по приведению процессов обработки персональных данных в соответствии с требованиями Закона о персональных данных

Компания «Инфосистемы Джет» имеет большой опыт по приведению в соответствие с нормативными документами ФСТЭК России и ФСБ России. Кроме того, компания обладает необходимым набором лицензий этих регулирующих органов по выполнению работ в части защиты конфиденциальной информации и государственной тайны.

Компания «Инфосистемы Джет» предлагает следующий перечень работ, направленных на приведение процессов обработки персональных данных в соответствии с требованиями закона:

1. Сбор информации о персональных данных (ПДн):
   - сбор информации о категориях и составе персональных данных, обрабатывающихся в организации, информационных системах (ИСПДн) и неавтоматизированных способах обработки персональных данных.
2. Сбор информации о защищенности персональных данных:
   - получение подробной информации о текущем состоянии защищенности ПДн;
   - выявление существующих угроз и уязвимостей, оценка показателей вероятности и ущерба для потенциальных угроз;
   - обследование существующих организационных и технических мер безопасности ПДн в организации в целом и в каждой ИСПДн в отдельности на соответствие требованиям безопасности ПДн и эффективности противодействия угрозам.
3. Составление адаптированной модели угроз для выявленных ИСПДн:
   - категорирование ПДн;
   - описание выявленных ИСПДн;
   - классификация типовых ИСПДн согласно РД ФСТЭК России для выбора типовых мер обеспечения информационной безопасности из каталога ФСТЭК России;
   - построение адаптированной модели угроз на основе методических рекомендаций ФСТЭК России с учетом списка угроз ИБ, выявленных на предыдущих подэтапах.
4. Подготовка классифицированных типовых и специальных ИСПДн к регистрации:
   - подготовка документов для регистрации операторов, классифицированных на предыдущих подэтапах ИСПДн в государственном реестре Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия.
5. Подготовка рекомендаций и плана-графика мероприятий по защите персональных данных в организации:
   - разработка рекомендаций и плана-графика мероприятий по защите ПДн во всех выявленных ИСПДн.

Необходимо отметить, что в данной статье речь идет только о консалтинговой деятельности. Поэтому в перечень не включены работы по созданию самих систем защиты персональных данных, их тестирование и внедрение, подготовка к сертификации средств защиты/аттестации ИСПДн в регулирующих органах и т.д. Таким образом, в области обеспечения соответствия Закону №152-ФЗ специалисты компании «Инфосистемы Джет» выполняют весь комплекс работ по защите персональных данных — от аудита до внедрения и сопровождения.

кации информационных систем ПДн, разработан и введен в действие комплект правовых актов и методических документов ФСТЭК России.

Для организаций соответствие закону будет дополнительным подтверждением перед зарубежными инвесторами и партнерами приверженности принятым европейским нормам, так как закон является поддержкой ранее ратифицированной в Российской Федерации, а именно в 2005 году, Европейской Конвенции 1981 года «О защите личности в связи с автоматической обработкой персональных данных». Помимо этого, соответствие закону облегчит взаимодействие российских организаций с европейскими партнерами, так как снимет ограничения, которые накладывает Директива 95/46/ЕС Евросоюза в части передачи ПДн только в страны, где действующие положения закона, как общие, так и частные, а также профессиональные нормы и меры безопасности, соответствуют принятым в стране происхождения персональных данных.

Отраслевые требования по информационной безопасности

Стандарт Банка России по обеспечению ИБ

Другим положительным примером изменения отношения государства к соблюдению норм в защите информации является стандарт Банка России, который регламентирует обеспечение ИБ в кредитно-финансовых организациях.

Полное наименование стандарта — «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2006. Стандарт распространяется на организации банковской системы Российской Федерации (далее БС РФ) и устанавливает положения (политики, требования и т.п.) по обеспечению информационной безопасности в организациях БС РФ. Положения настоящего стандарта применяются на добровольной основе.

Стандарт определяет:

- основные принципы обеспечения информационной безопасности организаций БС РФ;
- модели угроз и нарушителей информационной безопасности организаций БС РФ;
- политику информационной безопасности организаций БС РФ, ее состав и назначение, основные требования по обеспечению информационной безопасности, отображаемые в политиках информационной безопасности организации БС РФ;
- систему менеджмента информационной безопасности организаций БС РФ и модели зрелости процессов менеджмента информационной безопасности организаций БС РФ;
- цели и методы проверки и оценки информационной безопасности организаций БС РФ;
- направления развития стандарта.

Характерной особенностью стандарта СТО БР ИББС-1.0-2006 является определение модели зрелости информационной безопасности. Эта модель заимствована из стандарта CoBIT. Она представляет собой образец проработанности процессов менеджмента ИБ кредитно-финансовой организации. На основании приведенной в стандарте модели можно определить полноту, адекватность и эффективность процессов путем оценки их уровня зрелости.

Оценка уровня зрелости формируется совокупностью различных параметров для каждого из процессов. В стандарте, исходя из степени проработанности процессов, выделены пять уровней зрелости. Рекомендуемым является четвертый уровень, который характеризуется тем, что:

- разработана и совершенствуется нормативная и распорядительная документация по ИБ (политика ИБ, регламенты и положения ИБ, должностные инструкции персонала и т.п.);
- создана организационная структура управления ИБ. Четко определена ответственность персонала за деятельность, связанную с обеспечением ИБ;
- финансирование ИБ осуществляется по отдельной статье бюджета организации;
- есть назначенный куратор службы ИБ;
- осуществляется приобретение необходимых средств обеспечения ИБ;
- защитные меры (технические, технологические, организационные) встроены в АБС и банковские технологические процессы, непрерывно совершенствуются и основываются на хорошей практике. В процессе внедрения защитных мер используется анализ затрат и результатов, обеспечивается их оптимизация;
- последовательно выполняется анализ ИБ организации и рисков нарушения ИБ, а также возможных негативных воздействий;
- краткие занятия с работниками организации по вопросам обеспечения ИБ носят обязательный характер;
- введена аттестация персонала по вопросам обеспечения безопасности;
- проверки на возможность вторжения в АБС являются стандартизованным и формализованным процессом;
- осуществляется оценка соответствия организации требованиям ИБ;
- стандартизованы идентификация, аутентификация и авторизация пользователей. Защитные меры совершенствуются с учетом накопленного в организации практического опыта;
- уровень стандартизации и документирования процессов управления ИБ позволяет проводить аудит ИБ в достаточном объеме;
- процессы обеспечения ИБ координируются со службой безопасности всей организации;
- деятельность по обеспечению ИБ увязана с целями бизнеса;
- руководство организации понимает проблемы ИБ и участвует в их решении через назначенного куратора службы ИБ из состава высшего руководства организации.

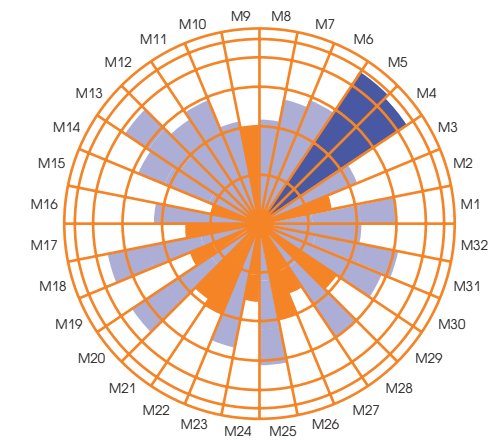
Обеспечение соответствия безопасности платежных систем требованиям стандарта PCI DSS

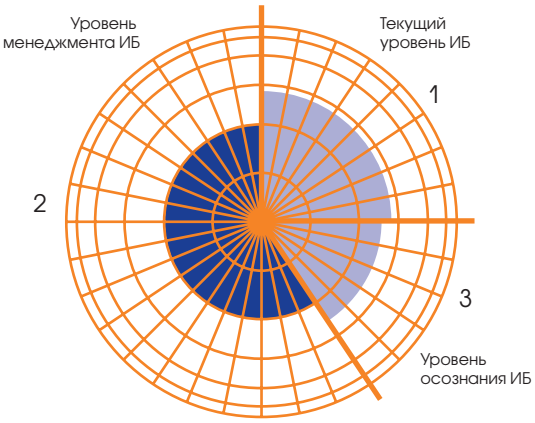
Одним из основных принципов российского законодательства в области ИБ является приоритет норм международного права над федеральным законодательством (если эти нормы не противоречат Конституции РФ). Это позволяет применять международные нормативно-правовые акты, которые относятся к лучшим мировым практикам, и таким образом покрывать недостатки и пробелы в российском законодательстве. Примером такой практики является применение в России стандарта Payment Card Industry Data Security Standard (PCI DSS).

Стандарт Payment Card Industry Data Security Standard (PCI DSS) разработан международными платежными организациями American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., объединившимися в консорциум PCI Security Standard Council (PCI SSC). Стандарт определяет требования к состоянию защищенности платежных систем кредитно-финансовых организаций, которые обрабатывают, хранят или передают информацию о держателях платежных карт. Такие структуры должны ежегодно подтверждать соответствие защищенности своих платежных систем требованиям стандарта PCI DSS путем прохождения сертификационного аудита, который могут выполнять только специализированные компании, обладающие соответствующим статусом:

- Qualified Security Assessor (QSA) (проведение сертификационного аудита);
- Approved Scanning Vendor (ASV) (внутреннее и внешнее сканирование ПС организации).

С 2006 года консорциум PCI SSC постепенно вводит систему штрафов, которые будут взыскиваться с финансовых организаций, если защищенность их платежной системы не соответствует требованиям стандарта PCI DSS.





Удовлетворительный уровень:
- Антивирусная защита
- Доступ к сети Интернет

Незначительные недостатки:
- Непрерывность бизнеса
- Принятие решений по рискам
- Анализ эффективности ОИБ руководством

Проблемные области:
- Управление рисками
- Обеспечение ИБ на всех этапах жизненного цикла АБС
- Совершенствование ИБ
- Мониторинг событий ИБ

текущий уровень ИБ: 0.69
менеджмент ИБ: 0.49
уровень осознания ИБ: 0.62

Итоговая оценка
0.49

Рекомендуемый ЦБ уровень
0.85

Рис. 3 Примеры оценки соответствия уровня ИБ стандарту СТО БР ИББС-1.0-2006

Предложение компании «Инфосистемы Джет»: «Консалтинг в области СТО БР»

Целевая аудитория
Услуга, как правило, заказывается кредитно-финансовыми организациями всех типов (например, коммерческих, государственных), разного масштаба и в том случае, когда есть необходимость оценить степень соответствия текущего уровня ИБ в компании требованиям стандарта Банка России СТО БР ИББС-1.0-2006.

Назначение услуги
Приведение применяемых в организации процессов управления ИБ, средств и методов защиты информации в соответствие с требованиями стандарта Банка России СТО БР ИББС-1.0-2006.

Задачи, решаемые в ходе проведения работ по данной услуге :

- оценка соответствия требованиям стандарта Банка России СТО БР ИББС-1.0-2006 по методике, разработанной специалистами компании «Инфосистемы Джет»;
- разработка рекомендаций по выполнению требований стандарта Банка России и созданию системы менеджмента информационной безопасности (СМИБ[7]);
- подготовка к аудиту на соответствие требованиям стандарта Банка России.

Состав работ:

- оценка соответствия СТО БР ИББС-1.0-2006
  - сбор основной информации о процессах обеспечения ИБ;
  - сбор информации о защищенности ИС;
  - оценка соответствия существующих средств и методов защиты информации требованиям стандарта;
- подготовка рекомендаций плана мероприятий по выполнению требований стандарта.

Результатом работ является отчет по анализу рисков состоящий из нескольких разделов:

- описание обследованных АС и сервисов;
- описание применяемых административных, организационных мер по обеспечению ИБ;
- описание применяемых программно-технических средств обеспечения ИБ;
- оценка степени соответствия применяемых в ИС банка мер и средств защиты информации требованиям стандарта СТО БР ИББС-1.0-2006;
- рекомендации по применению комплекса административных, организационных мер и программно-технических средств, направленных на устранение выявленных уязвимостей, включающие оценку стоимости внедрения рекомендуемых организационных мер и программно-технических средств.

Оптимизация системы обеспечения ИБ

Построение системы управления ИБ

Согласно международному стандарту ISO/IEC 27001:2005, система управления информационной безопасностью[8] (СУИБ) — это «часть общей системы управления организации, основанной на оценке бизнес-рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». СУИБ включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Целями создания системы управления информационной безопасности являются:

- построение эффективной системы обеспечения безопасности важнейшей корпоративной информации;
- обеспечение прозрачности процессов информационной безопасности;
- защита основных активов и критичных бизнес-процессов организации;
- минимизация рисков информационной безопасности при ведении операционной деятельности организации;

7 СМИБ: часть общей системы менеджмента организации банковской системы Российской Федерации, основывающаяся на подходе бизнес-риска. Предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации банковской системы Российской Федерации [ISO/IEC IS 27001].

8 В различных источниках такая система может называться по-разному. Существует два устоявшихся названия: «Система управления информационной безопасностью» (сокращенно СУИБ) и «Система менеджмента информационной безопасности» (сокращенно СМИБ).

Предложение Компании «Инфосистемы Джет» по консалтингу в области PCI DSS

Компания «Инфосистемы Джет» обладает всем необходимым (наличие QSA и ASV[9] статусов, квалифицированных специалистов и опыта проведения подобных проектов) для того, чтобы осуществлять консалтинг в области защиты платежных систем в соответствии со стандартом PCI DSS. Специалистами компании разработан соответствующий комплект услуг.

В отличие от других консалтинговых компаний, «Инфосистемы Джет» при проведении работ по консалтингу в области PCI DSS основной акцент делают не на проведение аудитов, целью которых является констатация факта соответствия или несоответствия стандарту, а на подготовку организации к сертификационному аудиту, то есть на построение эффективной системы защиты данных о держателях платежных карт.

Назначение услуги

Приведение применяемых в организации средств и методов защиты информации в соответствие с требованиями международного стандарта PCI DSS, разработанного в целях повышения уровня обеспечения безопасности в индустрии платежных карт. Распространяется не на всю организацию, а на системы, в которых производится обработка, передача или хранение данных о кредитных картах и их атрибутах.

Задачи, решаемые в ходе проведения работ по данной услуге:

1. Обследование на соответствие PCI DSS с выдачей детальных рекомендаций по подготовке к сертификационному аудиту (для тех, кто хочет понять, в чем несоответствие стандарту, и оценить/запланировать мероприятия по приведению в соответствие).
2. Подготовка к сертификационному аудиту (для тех, кто прошел обследование и принял решение выполнять работы по соответствию стандарту):
   - консультации;
   - разработка рабочих документов, необходимых для прохождения сертификации.

   Необходимо отметить, что в данной статье речь идет только о консалтинговых работах. Поэтому в перечень не включены работы по внедрению и поддержке специализированных программно-технических средств. Таким образом, в области обеспечения соответствия PCI DSS специалисты компании «Инфосистемы Джет» выполняют весь комплекс работ по защите платежных систем — от аудита до внедрения и сопровождения
3. Проведение сертификационного аудита с разработкой отчетов для регуляторов (соответствующая платежная система из состава консорциума PCI SSC).

- обеспечение непрерывности основной деятельности организации;
- выполнение нормативно-правовых требований к обеспечению информационной безопасности;
- повышение общего уровня управляемости организации за счет создания и интеграции системы управления информационной безопасности;
- облегчение процедуры выхода на IPO вследствие упрощения прохождения 3-й стадии — «technical due diligence». Повышение стоимости акций и снижение затрат на их размещение за счет выполнения требований по управлению операционными рисками.

Помимо этого, наличие сертификата соответствия ISO/IEC 27001:2005 подтверждает качество СУИБ, что в свою очередь сказывается на повышении стоимости бренда, особенно если речь будет идти о слиянии или покупке компании. Потенциальный собственник предпочитает знать, какие инструменты используются для управления безопасностью, ценит прозрачность системы информационной безопасности.

Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления. Используемый в ISO/IEC 27001:2005 для описания СУИБ, процессный подход предусматривает непрерывный цикл мероприятий, направленных на построение эф-

9 Для того чтобы пройти сертификацию на соответствие стандарту PCI DSS, кредитно-финансовая организация должна:
1. Проходить ежегодный сертификационный аудит. Ежегодный аудит должна проводить аккредитованная компания, имеющая статус QSA.
2. Проводить ежеквартальное сканирование. Сканирование должна проводить аккредитованная компания, имеющая статус ASV.
3. Проводить каждый год тест на проникновение (Penetration testing). Данные работы может проводить сама организация.

фективной системы управления ИБ: планирование, внедрение, проверка и улучшение СУИБ.

Одним из основных принципов создания подобной структуры управления является приверженность руководства. Это означает, что такая структура может быть создана только руководством компании, которое распределяет должности, ответственность и контролирует выполнение обязанностей. Иными словами, руководство организации строит соответствующую вертикаль управления для удовлетворения потребностей организации в безопасности.

Другим основополагающим принципом является вовлечение в процесс обеспечения ИБ всех сотрудников компании, имеющих дело с информационными ресурсами. Неосведомленность конкретных людей, работающих с информацией, отсутствие программы обучения по ИБ — одна из основных причин неработоспособности конкретных систем управления.

Не менее важно и то, что в основе создания СУИБ должен лежать анализ рисков ИБ. Отсутствие в организации процесса управления рисками приводит к неадекватности принимаемых решений и неоправданным расходам. Процесс управления рисками является основой, на которой строится система управления ИБ.

Столь же фундаментальным принципом является активное участие во внедрении и поддержке СУИБ специалистов заказчика. Привлечение внешних консультантов на всех этапах внедрения, эксплуатации и совершенствования СУИБ во многих случаях вполне оправдано. Более того, это является одним из механизмов контроля, описанных в ISO/IEC 27001:2005. Однако создание СУИБ без активного привлечения сотрудников самой компании невозможно по определению, т.к. СУИБ — это совокупность организационных структур, формируемых руководством, и процессов, реализуемых ее сотрудниками, которые должным образом осведомлены о своих обязанностях и обучены навыкам обращения с информацией и ее защитой.

Построение СУИБ представляет собой внедрение вертикально-интегрированных процессов обеспечения информационной безопасности, основными из которых являются:

- анализ рисков информационной безопасности;
- внутренние аудиты в области информационной безопасности;
- управление корректирующими/предупреждающими действиями;
- мониторинг эффективности процессов СУИБ;
- анализ функционирования СУИБ со стороны руководства;
- управление инцидентами информационной безопасности;
- управление непрерывностью бизнеса;
- организация обучения и осведомленности в области ИБ персонала;
- управление документацией СУИБ;
- управление записями СУИБ.

Работы по созданию СУИБ проводятся в четыре основных этапа:

1. Обследование, обнаружение и анализ степени соответствия требованиям стандарта ISO/IEC 27001:2005.
2. Создание СУИБ (разработка процессов) в соответствии с требованиями стандарта ISO/IEC 27001:2005.
3. Внедрение процессов СУИБ и подготовка СУИБ к сертификации.
4. Сертификация СУИБ[10] (при необходимости подтверждения качества системы).

Обследование, обнаружение и анализ соответствия требованиям стандарта ISO/IEC 27001:2005

На данном этапе осуществляются следующие работы:

- уточнение и предварительное согласование области деятельности[11] СУИБ;
- решение организационных вопросов по взаимодействию внутри компании и с исполнителем для успешной разработки и внедрения процессов;
- проведение обследования с целью выявления степени соответствия существующих организационных процедур и программно-технических средств защиты информации требованиям стандарта ISO/IEC 27001:2005 (так называемый GAP-анализ);
- формирование перечня необходимых доработок, выполнение которых позволит создать СУИБ, отвечающую требованиям стандарта ISO/IEC 27001:2005.

Область деятельности СУИБ

Построение системы управления информационной безопасности начинается с определения области (далее ОД) деятельности СУИБ. ОД представляет собой выделенную область организации, в кото-

10 Работы по сертификации созданной СУИБ выполняются соответствующим международным органом по сертификации и не входят в работы, выполняемые компанией-консультантом.

11 Стандарт применяется к выбранному организацией набору бизнес-процессов, который важен для основного бизнеса компании, определяемый в стандарте как область деятельности (ОД) СУИБ (см. раздел «Область деятельности СУИБ»).

рой внедряются процессы управления информационной безопасностью, подаваемые на сертификацию в соответствии с требованиями стандарта ISO/IEC 27001:2005. Область деятельности должна покрывать критичные для компании бизнес-процессы и сервисы и включать те подразделения, которые задействованы в выполнении данных процессов.

Примерами ОД СУИБ могут быть:

1. Для промышленных предприятий:
   - сегмент автоматизированных расчетов с клиентами;
   - процессы работы с поставщиками сырья или комплектующих;
   - процесс разработки новых продуктов и технологий;
   - ERP-системы (в данном случае не сама ERP-система, а критически важный бизнес-процесс, связанный с работой системы, например, поддержка ее работоспособности);
   - другие.
2. Для телекоммуникационных компаний:
   - сегмент автоматизированных расчетов с клиентами (биллинг);
   - службы электросвязи;
   - сети передачи данных;
   - ERP-системы;
   - другие.
3. Для кредитно-финансовых организаций:
   - процессы, связанные с автоматизированными банковскими системами (АБС);
   - процессы, связанные с автоматизированными платежными системами (процессинг);
   - процессы, связанные с автоматизированными системами межбанковского взаимодействия;
   - другие.

От того, насколько точно будет определена область деятельности, зависит эффективность внедрения системы управления информационной безопасности. Поэтому при проведении проектов по построению СУИБ данному этапу уделяется особенное внимание. При выборе ОД в расчет должны приниматься все важнейшие параметры, которые оказывают влияние на существование целевой корпоративной информации на всем ее жизненном цикле, а именно:

- непосредственная деятельность организации;
- продукты, сервисы или услуги, производимые организацией и предоставляемые клиентам;
- целевая информация, безопасность которой должна быть обеспечена при создании СУИБ;
- основные бизнес-процессы, в ходе которых создается, накапливается, обрабатывается, хранится и передается целевая информация;
- подразделения и сотрудники, задействованные в данных бизнес-процессах;
- программно-технические средства, обеспечивающие функционирование данных бизнес-процессов, в том числе средства защиты информации;
- территориальные площадки организации, на которых происходит сбор, обработка и передача целевой информации.

Решение организационных вопросов

Для того, чтобы правильно организовать процесс создания системы управления информационной безопасности и избежать проблем и конфликтных ситуаций в ходе выполнения проекта, необходимо уже на этапе подготовки решить ряд организационных вопросов.

Первым организационным мероприятием является издание приказа об открытии внутреннего проекта по созданию СУИБ. Данный приказ придает проекту статус общекорпоративного и определяет порядок взаимодействия различных подразделений в ходе его реализации.

Далее проводится назначение основных ролей в рамках СУИБ, которое позволит определить лиц, ответственных за ее создание. Эти сотрудники будут наделены определенным статусом и на них будут возложены обязанности, соответствующие их роли.

Иногда бывает необходимо, с целью придания проекту значимости, создать комитет СУИБ, в состав которого могут входить высшее руководство организации, руководители основных функциональных и вспомогательных подразделений. Комитет СУИБ принимает стратегические решения и утверждает основные документы, разработанные в ходе проекта.

Обязательным шагом является организация рабочей группы по реализации проекта по созданию СУИБ. Эта группа также может включать представителей высшего руководства компании с уже выделенными ролями в рамках СУИБ, владельцев бизнес-процессов, входящих в область деятельности СУИБ, ответственных сотрудников по внедрению СУИБ. Рабочую группу необходимо утверждать на высшем уровне для обозначения значимости данной системы и ее роли в организации. Рабочая группа осуществляет оперативную деятельность в ходе проекта.

Обследование с целью выявления несоответствий

На стадии проведения обследования осуществляется сбор и анализ информации о следующих регламентах, процедурах и средствах обеспечения ИБ,

используемых в рамках функционирования ИС организации:

- регламенты и процедуры существующих систем менеджмента (система менеджмента качества, другие системы управления, применяемые в компании, включая корпоративные стандарты управления);
- формализованные описания бизнес-процессов, охватываемых областью деятельности;
- инфраструктура сетевого и информационного взаимодействия;
- нормативная документация компании в области информационной безопасности (политика ИБ, регламенты и процедуры ИБ, положения по ИБ в эксплуатационных регламентах);
- организационное взаимодействие подразделений и ответственных лиц заказчика;
- организационно-распорядительная документация в области информационной безопасности (приказы, распоряжения, должностные инструкции и т.п.);
- перечень сведений, составляющих конфиденциальную информацию заказчика и подлежащих защите;
- сведения о применяемых мерах и средствах управления доступом пользователей к информационным ресурсам в соответствии с категориями ресурсов;
- сведения о результатах проводившихся в компании работ по анализу и управлению рисками, включая сведения о наличии процедур и инфраструктуры по анализу и управлению рисками;
- сведения об обучении пользователей, включая внутрикорпоративное обучение правилам обеспечения ИБ, а также внешнее обучение сотрудников правилам и методам обеспечения ИБ;
- сведения об организации процесса приема на работу и увольнения сотрудников;
- сведения об организации физической защиты площадок размещения программно-технических средств ИС, а также самих этих средств;
- технологические процедуры и инструкции по эксплуатации систем;
- сведения об организации процессов развития ИТ-инфраструктуры компании в целом и в части, касающейся концепции ИТ, порядка внесения изменений в эксплуатируемые системы, порядка закупок оборудования и ПО и т.п.;
- сведения об используемых средствах защиты информации в ИС заказчика;
- сведения об организации процедур резервного копирования и восстановления информации в ИС заказчика;
- сведения о применяемых в компании процедурах и планах по обеспечению непрерывности критичных бизнес-процессов и поддерживающих их систем;
- сведения о применяемых в компании процедурах защиты носителей информации и конфиденциальных документов;
- сведения о применяемых мерах по защите внешнего информационного обмена;
- сведения о применяемых средствах контроля действий пользователей;
- сведения об организации процессов разработки и модификации программного обеспечения;
- сведения об организации процессов периодической проверки (аудита) процессов обеспечения информационной безопасности и настроек технических средств защиты информации;
- сведения об организации процессов управления инцидентами, связанными с ИБ.

Далее в ходе обследования проводится интервьюирование руководителей структурных подразделений, а также лиц, ответственных за функционирование ИС и сопровождение отдельных ее компонентов в рамках области деятельности.

На основании полученных сведений разрабатывается детальный план-график выполнения работ по построению СУИБ.

Результатом этого этапа являются следующие данные:

- отчет о степени соответствия требованиям стандарта ISO/IEC 27001:2005;
- рекомендации по достижению требований стандарта ISO/IEC 27001:2005;
- план-график работ с распределением ответственности как специалистов интегратора, так и сотрудников самой организации на каждом этапе внедрения СУИБ.

Создание СУИБ в соответствии с требованиями стандарта ISO/IEC 27001:2005

На данном этапе осуществляются следующие работы:

- окончательное определение и утверждение области деятельности СУИБ, распланированные организационные мероприятия по внедрению СУИБ
- выбор подхода и проведение анализа рисков ИБ;
- определение ролевой структуры СУИБ и разработка полного комплекта документации СУИБ;
- формализация бизнес-процессов в рамках утвержденной области деятельности СУИБ;

- осуществление запланированных на начальном этапе организационных мероприятий по внедрению СУИБ.

Окончательное определение и утверждение на уровне высшего руководства документа «Область деятельности СУИБ» является начальным этапом в создании системы управления информационной безопасностью, после которого начинаются работы по выбору подхода и проведению процесса анализа рисков ИБ.

Выбор подхода и проведение анализа рисков ИБ

Анализ рисков ИБ[12] — это основной движущий процесс СУИБ. Он выполняется не только при создании СУИБ, а проводится на регулярной основе и при изменении бизнес-процессов организации и требований по безопасности.

Для проведения анализа рисков ИБ разрабатывается специальная методика. Она создается с учетом специфики организации.

К особенностям методики анализа рисков ИБ при создании СУИБ можно отнести:

- процессы идентификации активов и определения их ценности обязательно должны проводиться при участии владельцев бизнес-процессов организации;
- подход к анализу рисков «от активов»;
- в методике описывается, чем необходимо руководствоваться при принятии решения о приемлемом уровне риска;
- методика утверждается только на уровне высшего руководства;
- методика может включать в себя перечень угроз, применимых для организации, либо ссылаться на запись, содержащую данные угрозы. Перечень угроз утверждается на уровне высшего руководства.

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

Последний вариант наиболее предпочтителен, поскольку на данный момент 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 др.;
- 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 методике 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.

Результатом этапа анализа рисков ИБ является выбранный комплекс механизмов контроля, направленный на противодействие выявленным рискам, для которых было принято решение об их снижении. При этом высшим руководством организации утверждаются следующие документы:

- план обработки рисков;
- положение о применимости механизмов контроля.

12 Подробное описание работ приведено в разделе «Анализ рисков ИБ» данной статьи.

Мероприятия по снижению рисков проводятся силами и средствами заказчика с подробными консультациями со стороны компании-консультанта на этапе внедрения СУИБ.

Определение ролевой структуры СУИБ и разработка полного комплекта документации СУИБ

На данной стадии производится определение ролевой структуры СУИБ, ключевых ответственных за проект лиц, распределение обязанностей и формальное описание ролей в части СУИБ. В рамках области деятельности определяется формальный процесс назначения ролей специалистам и порядок внесения изменений в существующую ролевую структуру.

Разработка документации СУИБ производится специалистами исполнителя с привлечением специалистов заказчика в оговоренном объеме.

Результатом данной стадии являются следующие документы:

- Политика СУИБ;
- Процедура управления документацией СУИБ;
- Процедура управления записями СУИБ;
- Процедура проведения внутренних аудитов СУИБ;
- Процедура управления корректирующими действиями;
- Процедура предупреждающих действий;
- Процедура управления инцидентами ИБ;
- Процедура мониторинга эффективности СУИБ;
- Процедура анализа функционирования СУИБ руководством Компании;
- Положение о ролевой структуре СУИБ.

Разработка перечня документов, который необходимо разработать в соответствии с требованиями Приложения А[13] стандарта ISO/IEC 27001:2005, происходит после обследования состояния ИБ, как и определение степени доработки уже существующей в организации документации по ИБ.

Формализация бизнес-процессов в рамках области деятельности СУИБ

На данной стадии в рамках области деятельности проводятся следующие работы:

- описание высокоуровневых бизнес-процессов, потоков данных со смежными подразделениями, владельцев высокоуровневых бизнес-процессов;
- интервьюирование ответственных сотрудников организации (руководства, специалистов по оптимизации бизнес-процессов и т.д.) для получения полной информации о бизнес-процессах области деятельности, входах, выходах, механизмах управления и контроля;
- составление и согласование карты описания бизнес-процессов организации;
- выдача рекомендаций по доработке рабочих, операционных инструкций в рамках описанных бизнес-процессов области деятельности СУИБ.

Выбор средств описания бизнес-процессов области деятельности СУИБ согласуется после проведения обследования состояния ИБ. Работы по описанию бизнес-процессов могут осуществляться параллельно работам по проведению анализа рисков и разработке документации.

Результатом данной стадии являются:

- документ, описывающий карту бизнес-процессов в рамках области деятельности СУИБ, отвечающий требованиям стандарта ISO/IEC 27001:2005;
- рекомендации по дополнительному документированию операционных процедур в рамках области деятельности СУИБ.

Внедрение процессов СУИБ и подготовка СУИБ к сертификации

Внедрение процессов СУИБ и подготовка СУИБ к сертификации производится за счет реализации следующих работ:

- консультации по выполнению персоналом заказчика, вовлеченным в процесс функционирования СУИБ, своих должностных обязанностей в соответствии с изданной организационно-распорядительной и нормативной документацией;
- контроль и первичный запуск всех процессов СУИБ;
- помощь в документировании записей СУИБ в соответствии с подготовленными процедурами;
- обучение персонала заказчика, ответственного за разработку и внедрение СУИБ, с учетом разработки курса обучения, программы обучения, и с предоставлением специалистов исполнителя в качестве ключевых преподавателей;
- оказание консультаций по функционированию и взаимосвязям всех вновь разработанных процессов СУИБ.

13 Стандарт ISO/IEC 27001:2005 состоит из основной части, выполнение требований которой обязательно, и Приложения А, выполнение требований которого определяется по результатам анализа рисков ИБ.

Результатами данного этапа являются:

- утвержденный набор документации, необходимой для прохождения сертификационного аудита;
- персонал, обученный вопросам СУИБ в рамках области деятельности;
- набор записей, необходимый для прохождения сертификационного аудита (при этом сотрудники заказчика также будут обучены самостоятельному сбору и ведению записей);
- материалы для обучения персонала в части ИБ и тесты по ИБ.

Данный этап продолжается до второй стадии сертификационного аудита.

Сертификация СУИБ

Сертификация СУИБ по сути является итоговой проверкой формального соответствия ISO/IEC 27001:2005 (см. Рис. 4), производится сертификационными органами, которые владеют эксклюзивным правом выдачи сертификатов и имеют аккредитацию при UKAS (United Kingdom Accreditation Service) — уполномоченном государственном органе Великобритании. Такой компанией в России, например, является BSI Management Systems.

Сертификационный аудит, проводимый BSI Management Systems, как правило, включает в себя две стадии. На первой стадии проводится аудит документации. Он представляет собой изучение ключевых элементов СУИБ и осуществляется на территории организации.

Вторая стадия — аудит внедрения, который заключается в изучении и анализе политик, процедур и процессов. Главная его цель — это подтверждение эффективности внедренного в организации

Подход компании «Инфосистемы Джет» к построению СУИБ

Построение корпоративной СУИБ — это сложный, многоэтапный, циклический организационно-технологический процесс. Большое значение при построении СУИБ имеет наличие опыта в данной области, которым в полной мере обладает компания «Инфосистемы Джет». Из десяти сертифицированных организаций в России три подготовлены для сертификации компанией «Инфосистемы Джет»: ОАО «Межрегиональный ТранзитТелеком», ОАО «РОСНО», компания «Центр Безопасности Информации». Помимо этого «Инфосистемы Джет» обладают компетенцией сертифицированного партнера BSi Management System и имеют в штате проектную команду, включающую девять сертифицированных специалистов, из которых трое имеют статус преподавателя, двое — право проведения сертификационных аудитов.

При реализации проектов по созданию СУИБ специалисты компании «Инфосистемы Джет» особое внимание уделяют процессу внедрения системы, поскольку именно от качества внедрения зависит эффективность функционирования системы управления ИБ.

Существуют случаи, когда организация не обладает достаточными ресурсами для создания СУИБ в рамках одного проекта. Тогда компания «Инфосистемы Джет» предлагает поэтапное внедрение отдельных процессов и механизмов контроля СУИБ. В частности, к наиболее востребованным процессам СУИБ относятся:

- процесс управления рисками ИБ;
- процесс управления непрерывностью бизнеса;
- процесс управления инцидентами ИБ.

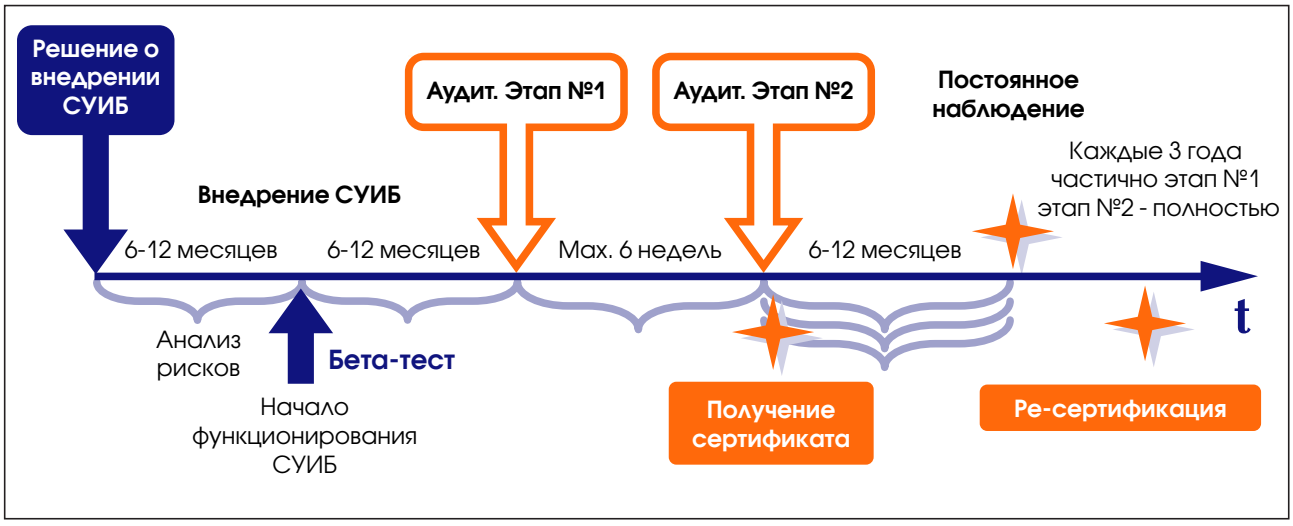


Рис. 4 Пример программы по созданию СУИБ и ее сертификации. Стадии и временные рамки.

Внедрение процесса управления непрерывностью бизнеса

Целевая аудитория
Услуга заказывается, когда в компании критична бесперебойная работа как ИТ-сервисов, так и всех служб компании в целом.

Назначение услуги
Услуга оказывается с целью создания процесса управления непрерывностью ИТ-сервисов организации, который строится в соответствии с требованиями стандартов BS 25999 и ISO/IEC 27001:2005.

Задачи, решаемые в ходе проведения работ по данной услуге
Основной задачей услуги является создание процесса непрерывности ИТ-сервисов в нештатных ситуациях.

Состав работ:
- обследование ИС заказчика;
- проведение анализа воздействия чрезвычайных ситуаций на ведение основной деятельности организации (Business Impact Analysis, BIA);
- разработка и внедрение планов аварийного восстановления ИТ-сервисов после сбоя (Disaster Recovery Plan, DRP) и планов обеспечения непрерывности ИТ-сервисов (Business Continuity Plan, BCP);
- разработка процедур непрерывности ИТ-сервисов и подготовка соответствующих документов, регламентирующих деятельность по обеспечению непрерывности ИТ-сервисов;
- тестирование DRP/BCP планов;
- обучение персонала организации процедурам непрерывности бизнеса.

Результатом работ является:
- работающий процесс непрерывности ИТ-сервисов;
- стратегия «Обеспечение непрерывности ИТ-сервисов»;
- планы восстановления ИТ-сервисов после сбоев;
- планы непрерывности ИТ-сервисов в нештатных ситуациях.

Внедрение процесса управления инцидентами ИБ

Назначение
Услуга оказывается с целью создания процесса управления инцидентами ИБ, который строится в соответствии с ISO/IEC TR 18044 и ISO/IEC 27001:2005.

Целевая аудитория
Компании, которые развиваются и по мере своего развития сталкиваются с проблемами увеличения ущерба от инцидентов ИБ, факт которых в большинстве случае даже не известен, а также с вопросами выбора и принятия адекватных решений, минимизирующих проблемы ИБ. Кроме того, услуга заказывается, когда в организации требуется не только реакция на инциденты, но и управление ими: анализ причин инцидентов, ведение статистики и т.п.

Задачи:
- определение области действия процесса;
- обследование существующего порядка управления инцидентами;
- разработка и внедрение процессов управления инцидентами информационной безопасности.

Состав работ
- Обследование объекта.
  На данном этапе осуществляется сбор и анализ информации об имеющихся и используемых на данный момент регламентах, процедурах и средствах обеспечения информационной безопасности и управления инцидентами. Выявляются источники событий ИБ, собираются сведения об используемых информационных системах и технологиях обработки данных. Определяется область действия процесса управления инцидентами информационной безопасности. Разрабатывается документ «Задание на работы по разработке процесса управления инцидентами информационной безопасности».
- Разработка процессов управления инцидентами ИБ.
  На втором этапе осуществляется разработка процессов управления инцидентами информационной безопасности, написание соответствующих документов (перечень которых задает «Задание на работы»).
- Третий этап — внедрение процессов управления инцидентами ИБ.
  На третьем этапе осуществляется внедрение процессов управления инцидентами информационной безопасности. Проводится обучение персонала, распределение ролей, интеграция процесса с другими процессами управления информационной безопасностью.

Результат работ
Формализованные процессы управления инцидентами ИБ.

СУИБ. Также проводится на территории организации.

Во время аудита СУИБ сертификационным органом организации оказывается помощь со стороны компании-консультанта. Она включает в себя следующие виды работ:

- оказание финальных консультаций перед проведением сертификации ключевых сотрудников области деятельности СУИБ;
- проведение контроля выполнения процессов СУИБ;
- присутствие на первой и второй стадии сертификационного аудита специалистов исполнителя;
- оказание консультаций по приведению в соответствие замечаний, наблюдений и несоответствий, выявленных на первой стадии сертификационного аудита, и разработка программы устранения несоответствий;
- внесение изменений в документацию и процессы СУИБ, в случае необходимости, исправления несоответствий до второй стадии сертификационного аудита;
- оказание содействия в разработке плана корректирующих/предупреждающих действий по результатам проведения второй стадии сертификационного аудита.

В случае, если организация не прошла сертификационный аудит, состав, сроки и условия выполнения работ после второй стадии определяются на момент завершения этапа сертификации СУИБ.

Результатом данного этапа являются отчеты со стороны сертификационного органа по итогам сертификационного аудита СУИБ.

Выводы

или Как не ошибиться с выбором консультанта?!

При создании или модернизации системы информационной безопасности компании часто обращаются за помощью к внешним консультантам. Как выбрать надежного партнера, которому можно было бы доверить одну из самых критичных областей бизнеса? Ведь выбор консалтинговой компании определяет успех не только в реализации какого-то одного проекта по ИБ, но и дальнейшее развитие организации.

Деятельность квалифицированного консультанта, предоставляющего услуги в области информационной безопасности, должна быть подчинена ряду требований, основными из которых являются:

- консультант (либо консалтинговая компания) обязан владеть методической базой и технологиями, необходимыми для выполнения работ. Важной составляющей здесь является наличие собственных комплексных методик аудита, построения СУИБ, анализа и управления рисками и т. п., которые бы включали в себя не только директивы международных стандартов в области ИБ, но и были бы расширены за счет использования собственного экспертного опыта по консалтингу в области ИБ;
- консультант (либо консалтинговая компания) должен быть независим от поставщиков продуктов и решений в избранной области, а также традиций, «неписаных законов» и политики управленческого аппарата организации заказчика. Мнение консультанта должно носить свободный и объективный характер;
- консультант (либо консалтинговая компания) должен являть собой структуру, внешнюю по отношению к консультируемой организации. Соблюдение этого принципа позволяет добиться объективности при решении множества важнейших задач консалтинга (например, оценка степени зрелости, определение направления развития и т.п.) в области информационной безопасности;
- консультант (либо консалтинговая компания) обязан оказывать заказчикам помощь в использовании их собственного опыта для непрерывного совершенствования деятельности в области информационной безопасности;
- консультант (либо консалтинговая компания) должен обладать достаточным опытом проведения работ не только по консалтингу в области ИБ, но и в предметной области, в отрасли, в которой работает заказчик услуг.

Одним из основных факторов, влияющих на выбор компании, оказывающей услуги по консалтингу в области информационной безопасности, является уровень доверия к консультанту. Это объясняется тем, что в большинстве случаев компании-консультанту предоставляется доступ к конфиденциальной информации заказчика, поэтому к ней предъявляются повышенные требования. Такой уровень доверия может быть обеспечен не только заключением соответствующих договоров о конфиденциальности и неразглашении сведений, которые станут известны консультанту в ходе работ по консалтингу, но и наличием необходимых лицензий государственных и регулирующих органов, предоставляющих право осу-

ществлять работы в области информационной безопасности.

Компания, оказывающая услуги консалтинга в области ИБ, должна иметь соответствующие партнерские статусы от ведущих вендоров на рынке информационной безопасности, при этом данный статус должен определять возможности компании не только по дистрибуции средств защиты, но и способности консультанта по внедрению и технической поддержке данных средств.

Преимуществом компании-консультанта является также наличие тесного взаимодействия с различными ассоциациями, органами по сертификации, разработчиками стандартов и требований в области ИБ. Это позволяет консультантам быть в курсе последних изменений и тенденций в области информационной безопасности, что соответственно повышает уровень их компетенций в вопросах ИБ. Примерами таких взаимодействий могут являться:

- членство и участие в работе ассоциации ABISS — сообщества пользователей стандартов Центрального Банка РФ по обеспечению информационной безопасности организаций банковской системы РФ, чья деятельность связана с развитием и продвижением Стандарта Банка России в области ИБ СТО БР ИББС-1.0 и связанных с ним стандартов;
- взаимодействие с международными платежными системами VISA и Master Card в части выполнения требований по приведению платежных систем организаций в соответствие требованиям стандарта PCI DSS. Данное взаимодействие со стороны компании-консультанта может быть в любой форме, в том числе и в форме аккредитации консалтинговой компании в качестве органа по сертификации по стандарту PCI DSS. Такая аккредитация, помимо права на проведение сертификационного аудита, позволяет понимать видение разработчиков стандарта и предлагать качественные услуги по консалтингу в данной области;
- партнерство с разработчиками международных стандартов, такими как компания BSI (Британский Институт Стандартов), позволяющее лучше понимать требования стандартов к системам менеджмента, в том числе и в области ИБ, и предлагать качественные услуги по созданию таких систем.

Принять решение о том, какую консалтинговую компанию выбрать для решения вопросов по информационной безопасности — непростая задача. Надеемся, что данная статья поможет многим организациям в ее решении.

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Шедова Е.Л. *(eshedova@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