Управление процессами ИБ в интересах бизнеса

Введение в Систему Автоматизации Процессов Управления Информационной Безопасностью (САПУИБ), разработанную компанией ООО "Газинформсервис" на платформе EMC RSA Archer eGRC и позволяющую жестко увязывать управление процессами информационной безопасности (ИБ) с бизнес-процессами компании, а также с требованиями региональных и отраслевых регуляторов.

Игорь Алексеевич Жуклинец – к.т.н., начальник отдела ООО "Газинформсервис".

Олег Николаевич Марков – к.т.н., руководитель группы разработки ООО "Газинформсервис".

Введение

Современные условия стабильного развития бизнеса компании немыслимы без автоматизации различных аспектов ее деятельности. Поэтому каждое предприятие, деятельность которого достаточно сильно зависит от информационных систем, рано или поздно сталкивается с необходимостью комплексного внедрения систем защиты информации и совершенствования процессов управления информационной безопасностью.

Как показывает опыт, большинство российских компаний при решении вопросов, связанных с обеспечением информационной безопасности, не учитывают влияние процессов обеспечения и управления ИБ на бизнес-процессы компании. Таким образом, отсутствует главное звено – бизнес-процессы (деятельность) компании – то ради чего создаются система защиты информации и система управления информационной безопасностью – видимо, поэтому многие руководители относятся к обеспечению ИБ, как к некой обособленной сущности, существующей в отрыве от производственной деятельности предприятия. И это является причиной нарушения одного из главных принципов функционирования системы управления информационной безопасностью компании: осознанная заинтересованность и вовлеченность высшего руководства компании в процессы управления ИБ.

Необходимо акцентировать внимание, что обеспечение информационной безопасности компании – это не разовая акция, а непрерывная деятельность по планированию, реализации, измерению и совершенствованию процессов обеспечения и управления ИБ. Это один из современных подходов к менеджменту, основанный на цикле Шухарта-Деминга (цикл PDCA – "Plan-Do-Check-Act").

Внедрение процессного подхода к управлению информационной безопасностью позволит на основе формализованной системы метрик оценивать эффективность функционирования процессов управления ИБ в компании с учетом множества факторов, таких как: поддержание в актуальном состоянии документационного обеспечения ИБ; определение критичности и текущего состояния защищенности активов компании; оценка рисков информационной безопасности и существующих защитных мер; работа с персоналом по вопросам ИБ; обработка инцидентов информационной безопасности; оценка соответствия требованиям собственным политикам ИБ и требованиям регуляторов в области ИБ и др.

Классификация процессов ИБ

С точки зрения целевого назначения, процессы ИБ классифицируются на процессы обеспечения и процессы управления. Процессы обеспечения ИБ предназначены для реализации непосредственных организационных и технических функций защиты объектов (технических средств, программного обеспечения и информационных активов). Процессы управления ИБ предназначены для реализации управляющих действий в отношении системы обеспечения ИБ (СОИБ).

К процессам обеспечения ИБ относятся:

- организация безопасной эксплуатации средств обработки, хранения и передачи информации;
- регистрация и учет событий ИБ;
- защита от вредоносного программного обеспечения;
- резервное копирование информационных ресурсов;
- защита сетевых сервисов и обеспечение сетевой безопасности;
- обеспечение ИБ при обращении со съемными носителями информации;
- защита программного обеспечения;
- криптографическая защита информации;
- контроль доступа;
- контроль защищенности и состояния ИБ.

К процессам управления ИБ относятся (с привязкой к циклу PDCA):

1. Процессы планирования (P - Plan):

- разработка (уточнение) политики ИБ организации;
- идентификация и классификация объектов защиты;
- оценка рисков;
- идентификация приемлемых рисков;
- обработка рисков и оценка остаточных рисков;
- выбор (уточнение) задач по реализации защитных мер и их обоснование для минимизации рисков;
- формирование плана обеспечения ИБ.

2. Процессы реализации (D - Do):

- реализация плана обеспечения ИБ;
- управление безопасностью, связанной с персоналом;

– обучение персонала по вопросам обеспечения ИБ;

– повышение осведомленности работников в вопросах обеспечения ИБ;

– управление инцидентами ИБ;

– обеспечение непрерывности деятельности организации и восстановление нормального функционирования после устранения последствий инцидентов ИБ;

– идентификация и анализ изменений, влияющих на СОИБ;

3. Процессы проверки (C - Check):

– проверка соответствия СОИБ принятым целям и действующей политике ИБ организации;

– оценка эффективности СОИБ и информирование руководства организации о состоянии дел по обеспечению ИБ;

– анализ СОИБ руководством организации;

4. Процессы совершенствования (A - Act):

– проведение корректирующих действий по совершенствованию СОИБ;

– принятие превентивных мер по обеспечению ИБ.

На внедрение системы управления информационной безопасностью в организации могут оказывать влияние такие факторы, как:

– наличие удаленных филиалов;

– большое количество персонала головного офиса и филиалов;

– значительный объем предъявляемых требований со стороны международных, отечественных, отраслевых и корпоративных стандартов и нормативных документов в области ИБ;

– наличие уже внедренных систем защиты информации;

– необходимость непрерывного и эффективного обеспечения и демонстрации соответствия комплексу требований по ИБ.

Понятно, что в условиях ограниченного штата подразделений ИБ, очень сложно создать, внедрить и поддерживать такую систему управления информационной безопасности для крупных организаций (например, от 500 автоматизированных рабочих мест) и имеющих филиальную структуру.

Указанные особенности обусловливают необходимость задействования средств автоматизации процессов управления ИБ. В частности, представляется затруднительным осуществление классификации объектов защиты или оценки рисков ИБ без средств автоматизации, учитывая сложность информационной инфраструктуры, большое количество прикладных систем, где обрабатывается информация ограниченного доступа, обширный перечень критичных ресурсов, подлежащих защите. Или же, например, внедрение и функционирование СУИБ с учетом процессного подхода требует обращения внутри системы значительного объема документов, что ведет к необходимости автоматизации документооборота СУИБ.

Система автоматизации процессов управления информационной безопасностью

ООО "Газинформсервис" в качестве технического решения предлагает Систему автоматизации процессов управления информационной безопасностью (САПУИБ), которая позволит:

– внедрить и автоматизировать процессный подход к управлению ИБ;

– осуществлять сбор и анализ информации по вопросам ИБ в единой системе (как ручной ввод, так и импорт из смежных систем);

– обеспечить информационно-технологическую поддержку деятельности сотрудников подразделений ИБ и ИТ.

САПУИБ реализуется на основе платформы RSA Archer. RSA Archer является лидером мирового рынка в классе IT-GRC (Governance, Risk and Compliance) and Enterprise GRC систем (по свидетельству Forrester Research Inc.).

С точки зрения использования RSA Archer eGRC как платформы разработки, она имеет следующие возможности (рис. 1):

– широкую функциональность встроенных модулей;

– удобный пользовательский интерфейс;

– единую среду взаимодействия сотрудников подразделений ИБ, ИТ, владельцев информационных активов и пользователей информационных систем по вопросам ИБ;

– формирования отчетов по требуемым формам;

– инструменты разработки для оперативной адаптации функциональности системы под требования заказчика;

– генерацию уведомлений о событиях системы пользователям;

– гибкие инструменты интеграции со смежными системами;

– механизмы ролевого разграничения доступа к функциональности системы;

– гибкие инструменты поиска информации.

Помимо платформы, RSA Archer GRC включает готовые решения и библиотеку контентного наполнения (шаблоны корпоративных политик, стандартов и процедур безопасности, авторизованные источники, опросные листы). Применение

Рис. 1. Возможности платформы RSA Archer eGRC для автоматизации управления информационной безопасностью.

решений и библиотеки RSA Archer GRC требует их локализации и адаптации под специфические особенности компании, индивидуальные требования заказчиков путем настройки интерфейсов, изменения функциональности и разработки новых приложений, дополняющих готовые решения. Если Заказчик опирается на принятую систему отраслевых или корпоративных стандартов и методик их применения, то требуется разработка собственных корпоративных решений.

Так для финансово-кредитных учреждений разработчиками ООО "Газинформсервис" предлагается решение по контролю соответствия требованиям ИБ, выполненное в соответствии со Стандартами Банка России в области ИБ:

– поддержка требований п. 8.13. СТО БР ИББС 1.0 - 2010 к процедуре проведения самооценки;

– расчет уровней соответствия ИБ выполнен по методике, изложенной в СТО БР ИББС-1.2-2010.

Примером заказной разработки выступает реализация САПУИБ, выполненная в соответствии с корпоративной системой нормативно-методических документов в области комплексных систем безопасности объектов ОАО "Газпром". Реализация САПУИБ включает содержательное наполнение нормативными и правовыми актами, нормативными и методическими документами, корпоративными нормативными и организационно-распорядительными документами в области ИБ, вопросами для определения уровня зрелости организации в области ИБ, оценки соответствия требованиям ИБ, определения уровня критичности активов.

САПУИБ на основе платформы RSA Archer GRC обеспечивает возможность развертывания территориально-распределенной системы, адаптацию под требования Заказчика и функциональную расширяемость в случае необходимости модернизации. Система строится на модульном принципе (рис. 2). Состав модулей соответствует основным процессам управления информационной безопасности:

– *модуль "Документационное обеспечение"* – автоматизирует хранение, согласование, определение актуальности документов в рамках процессов управления ИБ;

– *модуль "Учет и классификация объектов защиты"* – автоматизирует процедуры классификации и учета информационных систем и сервисов;

– *модуль "Работа с персоналом и третьими сторонами по вопросам ИБ"* – автоматизирует процедуры доведения корпоративной организационно-распорядительной документации по обеспечению ИБ до работников Общества, контроль знаний работниками Общества требований по ИБ;

– *модуль "Управление рисками ИБ"* – автоматизирует процедуры идентификации, анализа, оценки и обработки рисков;

– *модуль "Управление инцидентами ИБ"* – автоматизирует процедуры регистрации, обработки инцидентов ИБ, оповещения о них, хранения статистики и результатов расследования инцидентов ИБ;

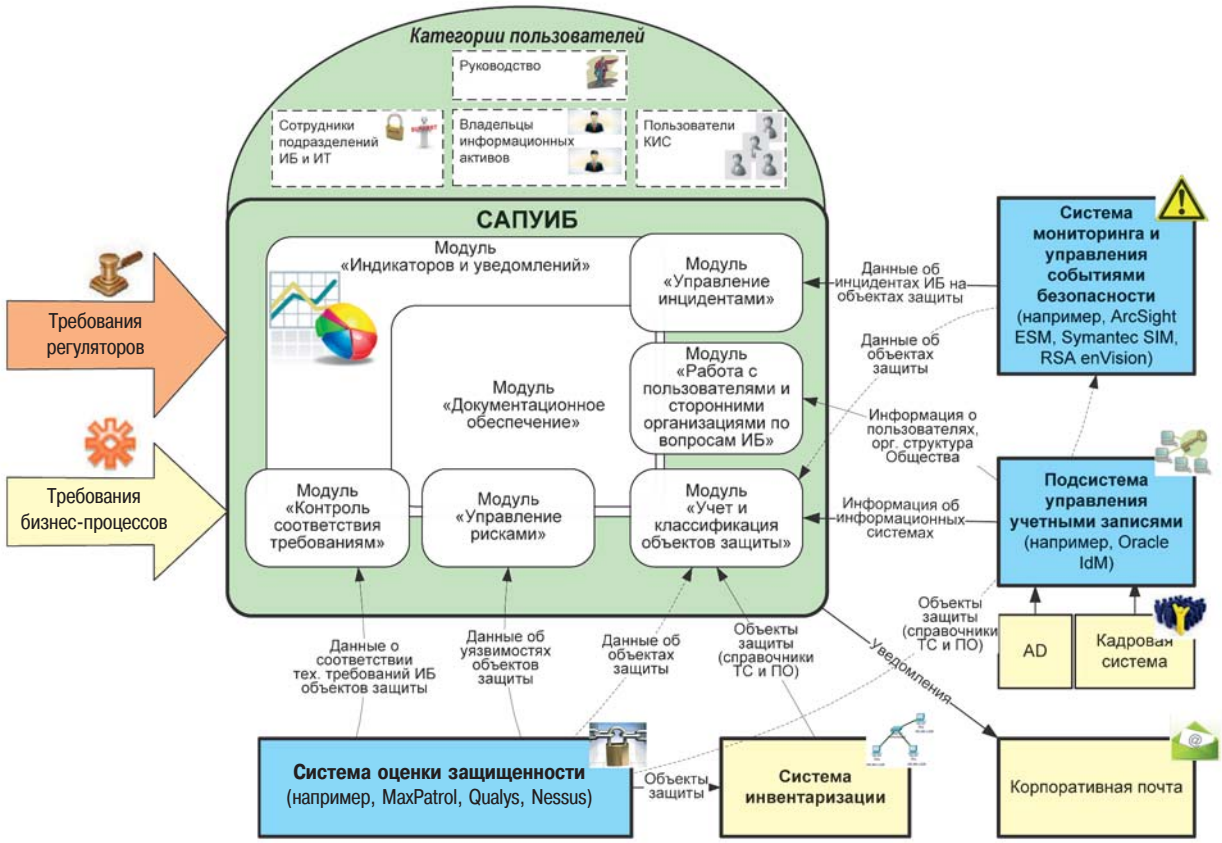

Рис. 2. Взаимодействие смежных информационных систем с модулями САПУИБ.

– *модуль "Контроль соответствия требованиям ИБ"* – автоматизирует процедуры самооценки соответствия системы СОИБ Общества требованиям по ИБ, определяемым законодательством Российской Федерации и корпоративными нормативными документами;

– *модуль "Индикаторы и уведомления"* – позволяет формировать уведомления участникам процессов о событиях управления ИБ и индикаторы, характеризующие эффективность функционирования процессов управления информационной безопасностью по данным обрабатываемым в модулях.

Состав модулей может быть расширен и адаптирован под конкретные условия применения, специфику деятельности и потребности заказчика. Все модули взаи-

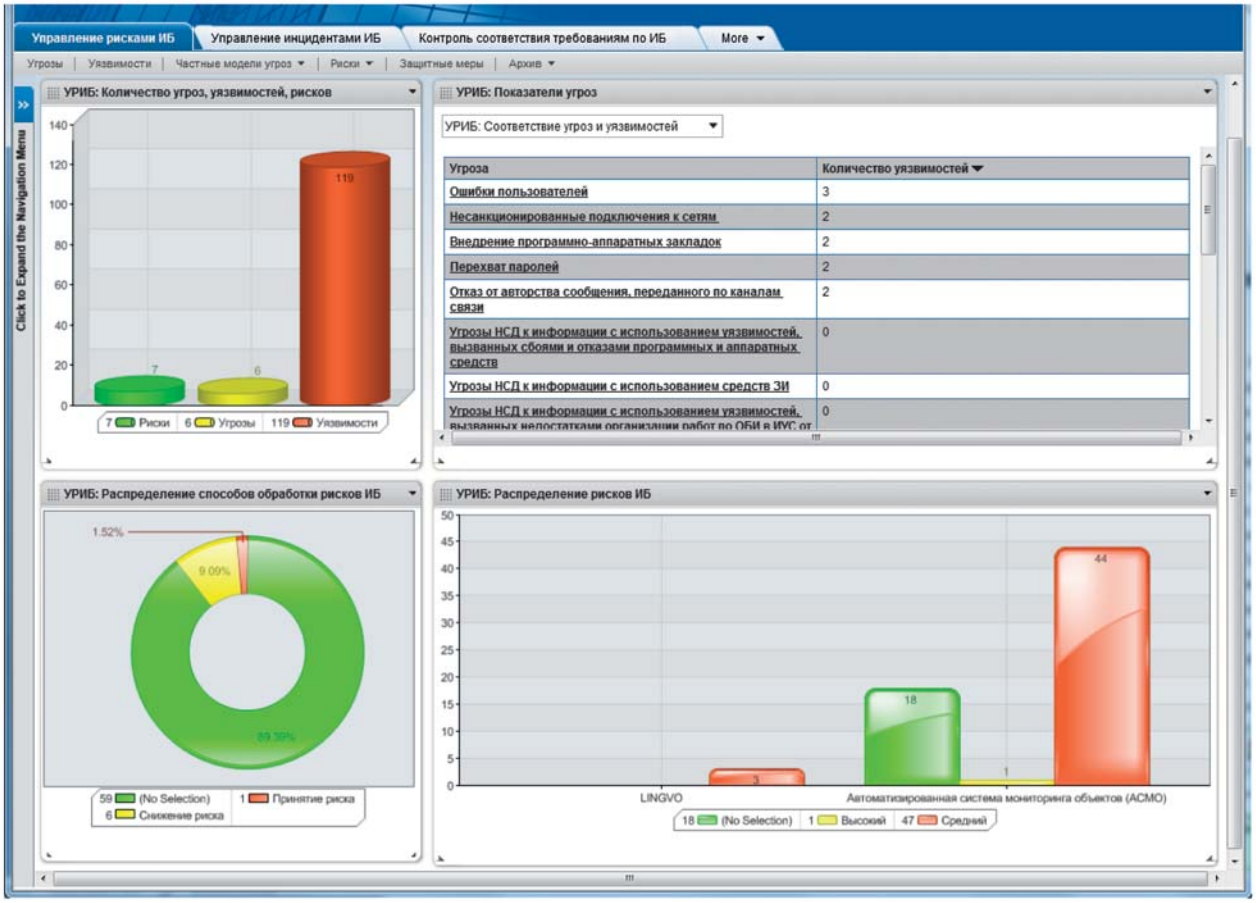

Рис. 3. Информационная панель модуля "Управление рисками".

моувязаны между собой в соответствии с логикой работы и используют единое хранилище данных. Так, модуль "Управление рисками ИБ", с одной стороны, использует результаты классификации объектов защиты, определяемые на основе их влияния на бизнес-процессы компании, с другой – использует статистику из модуля "Управление инцидентами ИБ" для определения вероятности возникновения угроз ИБ. В свою очередь, по результатам обработки рисков формируются задачи на разработку документов и планов обучения работников компании.

Система может внедряться целиком или последовательно по отдельным модулям, исходя из приоритетов задач, стоящих перед компанией.

САПУИБ имеет широкие возможности по интеграции с существующими средствами и системами защиты информации компании, в том числе с:

- системой оценки защищенности;
- системой мониторинга и управления событиями безопасности;
- подсистемой управления учетными записями;
- системой инвентаризации ИТ-инфраструктуры;
- системой корпоративной электронной почты.

Инструменты по интеграции RSA Archer eGRC с другими системами включают следующие механизмы:

- импорт данных в стандартных текстовых форматах (в том числе CSV, XML);
- импорт и экспорт данных с использованием распространенных протоколов взаимодействия (в том числе, LDAP, ODBC, POP3, SMTP, RSS, FTP, HTTP);
- взаимодействие на уровне прикладного программного интерфейса веб-сервисов для обеспечения тесной интеграции с иными программными продуктами с использованием протокола SOAP.

В основном, САПУИБ является потребителем информации для последующей ее обработки в интересах управления информационной безопасностью, но при необходимости может быть реализован и экспорт данных – это зависит от возможностей взаимодействующей системы. В качестве примера такого взаимодействия можно привести экспортный информационный поток задач на сканирование необходимых объектов из САПУИБ в MaxPatrol.

Каждый модуль содержит индикаторные панели наиболее важных отчетов, которые представляются в виде контекстно-зависимых графиков и диаграмм различных типов или табличных форм. Пример интерфейса модуля "Управление рисками ИБ" представлен на рис. 3.

Заключение

Внедрение САПУИБ позволит решать следующие задачи для структур компании:

- ***руководства**:*
  - *оптимизировать расходы на информационную безопасность за счет планирования внедрения мер обеспечения ИБ по результатам обработки рисков;*
  - *снижать операционные затраты за счет формализации и автоматизации процессов управления ИБ;*
  - *обеспечивать прозрачность деятельности подразделений ИБ и ИТ;*
- ***подразделений ИБ:***
  - *повышать эффективность процессов управления ИБ за счет достижения комплексности, взаимосвязанности, согласованности действий всех участников процессов обеспечения и управления ИБ на основе единых правил и консолидации информации;*
  - *обеспечивать оперативное предоставление в наглядной визуальной форме достоверной структурированной информации о текущей реальной защищенности информационных активов;*
  - *обосновывать расходы на информационную безопасность;*
  - *снижать затраты на контроль выполнения сотрудниками установленных корпоративных требований безопасности информации и соблюдения требований регуляторов;*
  - *получать аналитическую информацию для принятия решения по управлению ИБ;*
- ***подразделений ИТ:***
  - *интегрировать системы анализа защищенности, управления событиями и инвентаризации информационных ресурсов;*
  - *осуществлять реагирование на инциденты ИБ с учетом критичности объектов защиты;*
  - *обеспечить выполнение требований ITIL, COBIT в части IT-безопасности;*
- ***владельцев информационных активов, бизнес-процессов:***
  - *выявлять угрозы безопасности для бизнес-процессов;*
  - *обеспечивать защиту активов с учетом их критичности для бизнеса;*
- ***пользователей информационных систем и сервисов:***
  - *повышать осведомленность по вопросам обеспечения ИБ.*

Например, по нашим экспертным оценкам, внедрение только одного модуля "Учет и классификация объектов защиты" дает выигрыш не менее 200 чел./дней за счет автоматизации данного процесса управления ИБ для 3000 объектов защиты (технические средства, программное обеспечение и информационные активы) и не менее 50 чел./дней при последующей актуализации сведений.

Игорь Алексеевич Жуклинец,
Олег Николаевич Марков,
ООО "Газинформсервис".

Локализация решений RSA на базе платформы Archer

Александр Чигвинцев – руководитель подразделения EMC RSA в регионе Россия и СНГ.

Локализация решений RSA в составе любого ИТ-проекта по ИБ в соответствии с региональными и отраслевыми требованиями ИБ – один из наиболее важных моментов проекта. В этом плане платформа RSA Archer предоставляет практически неограниченные возможности как по адаптации готовых модулей (Audit Management, Policy Management, Risk Management и т.д.) к особенностям бизнес-процессов предприятия, так и по разработке собственных приложений GRC (Governance, Risk and Compliance) на базе предоставляемой программной инфраструктуры. При этом следует отдельно отметить, что создание собственных приложений не требует программирования, а фактически сводится к визуальному проектированию в модуле Application Builder.

Используя стандартный инструментарий RSA Archer, специалисты ООО "Газинформсервис" реализовали в рамках данной программной платформы специализированные решения в соответствии с корпоративной системой нормативно-методических документов в области комплексных систем безопасности объектов ОАО "Газпром". Компания RSA уверена, что положительный опыт создания ООО "Газинформсервис" локализованных решений на платформе Archer крайне важен для дальнейшего развития данной технологии и продвижения ее на российском рынке.