Самоаудит как инструмент управления безопасностью критических объектов и инфраструктур

В. П. Авдотьин, А. А. Кононов

Развитие процессов управления безопасностью все больше приводит к пониманию повышения важности совершенствования механизмов управления безопасностью и содействия становлению культуры безопасности.

И в этой связи особого внимания заслуживает такой инструмент, как самоаудит безопасности (САБ). Именно самоаудит безопасности может стать основой перевода всей экономики и, в первую очередь, критически важных объектов (КВО), на новый уровень безопасности и конкурентоспособности в условиях роста экономической свободы и самостоятельности хозяйствующих субъектов.

Самоаудит, внутренний аудит, или самооценка безопасности — это периодически выполняемые процедуры контроля защищенности предприятий, организаций, учреждений выполняемые собственными силами, либо по собственной инициативе с привлечением специализированных организаций.

Следует указать, что при желании можно пытаться определить семантические различия терминов «самоаудит», «внутренний аудит», или «самооценка» безопасности, но в данной работе предлагается считать их синонимами и далее использовать термин «самоаудит безопасности».

Самоаудит безопасности должен проводиться по некоторой заданной системе требований определенных во внутренних документах организации — в политике безопасности, приказах, инструкциях, руководствах, а также в законах, нормативных актах, стандартах, и других документах принятых регулирующими органами. Как минимум, система требований безопасности должна включать все те требования, по которым в организации могут осуществляться внешние проверки или аудит. Расширение системы требований возможно, если есть цель закрыть все выявленные риски и угрозы, даже те, защита от которых не предусмотрена в действующих нормативных документах.

Выделим три возможных схемы проведения САБ:

- самоаудит с построением и контролем модели угроз, модели защиты и оценкой рисков возможных потерь;
- самоаудит по заданным системам требований;
- контроль по заданным системам требований с контролем качества и адекватности требований.

Первая схема аудита — с построением и контролем модели угроз, модели защиты и оценкой рисков возможных потерь — требует достаточно высокой квалификации и достаточно высоких затрат, особенно на начальном этапе построения исходных модели угроз и модели защиты.

С другой стороны он позволяет получить модель защищенности системы и при ее последующем сопровождении лишь ее актуализировать по мере появления изменений, в том числе, в случаях выявления новых уязвимостей и новых угроз. Модель защищенности, включающая в себя взаимосвязанные перманентно актуализируемые модели угроз и защиты, является мощным инструментом контроля качества требований безопасности.

Эта схема может оказаться единственно возможной для уникальных объектов, для которых не существует готовых решений в виде законченных профилей защиты (систем требований), выполнение которых будет гарантировать защищенность от основных наиболее вероятных и опасных угроз. Также ее не удастся избежать, если построение моделей угроз и защиты предусмотрено используемой системой требований.

Вторая схема САБ — самоаудит по заданным системам требований — представляется более экономичной, поскольку, как правило, не требует построения и актуализации модели угроз и модели защиты, и в тоже время позволяет декларировать соответствие определенным системам требований, быть в состоянии постоянной готовности к внешним проверкам и внешнему аудиту по заданным системам требований. Однако если возникает необходимость доказывать невозможность, нецелесообразность или деструктивность выполнения отдельных требований безопасности, то такой доказательной базы, которая может быть приведена при наличии актуализированных моделей защищенности, может и не быть.

Третья схема САБ совмещает две предыдущие — это контроль по требованиям с контролем качества и адекватности системы требований.

Она предполагает, что осуществляется контроль по заданным системам требований, но помимо этого используются и приемы построения модели угроз и модели защиты, для того, чтобы верифицировать полноту, непротиворечивость, неизбыточность предполагаемых к выполнению систем требований. На первый взгляд такого рода схема представляется более затратной, чем схема самоаудита по заданным системам требований, но на самом деле она дает возможность разобраться с актуальностью требований, с их значимостью, определить требования выполнение которых является по сути избыточным, или невозможным в силу противоречия другим требованиям или в силу каких-либо иных причин.

Культивирование САБ, его внедрения в практику обеспечения безопасности, особенно на критически важных объектах, может дать целое множество преимуществ.

Прежде всего САБ позволяет добиваться реального выполнения требований безопасности конкретными исполнителями и тем самым снизить риски так называемого «человеческого фактора». Периодическое, по крайней мере, ежегодное, а на КВО — ежеквартальное, проведение самоаудита безопасности способствует лучшему усвоению требований безопасности, осознанию важности их выполнения. Как правило, соблюдение требований безопасности, требует дополнительных расходов сил и средств и поэтому очень часто возникает соблазн оптимизировать выполнение тех или иных задач, игнорируя требования безопасности. И такого рода тенденции усиливаются при отсутствии систематического контроля выполнения требований. И, наоборот, систематический периодический контроль выполнения требований безопасности способствует формированию культуры безопасности и рационализации деятельности.

В настоящее время подавляющее большинство предприятий, в том числе, и тех, что относятся к числу КВО, существуют в условиях ожесточенной конкурентной борьбы и жестких режимов экономии. Чтобы выжить они вынуждены развивать системы контроля качества и системы непрерывного совершенствования своей деятельности, такие как «шесть сигма». В этих условиях систематическое проведение самоаудита безопасности становится не только механизмом развития культуры безопасности, но инновационным механизмом, стимулирующим внедрение новых безопасных технологий и новых технологий обеспечения безопасности. Периодический самоудит безопасности способствует более глубокому осознанию проблем безопасности, что, в свою

очередь, выводит их в число первоочередных в критериальных системах принятия решений по техническому и технологическому развитию предприятий и организаций и способствует внедрению более безопасных технологий, а также новейших технологий безопасности.

Реальность сегодняшних дней такова, что те технологии, которые еще несколько лет назад казались неприемлемым решением из-за их дороговизны, становятся доступны и зачастую только инерция и недостаток мотивировочной базы сдерживает их использование на конкретных объектах. И именно объективный контроль безопасности, и в частности САБ, и выявление с его помощью недостатков и уязвимостей становятся тем недостающим основанием мотивов инновационных усилий в области повышения безопасности на основе новейших технологий.

Самоаудит безопасности может стать реальным конкурентным преимуществом. Периодический всесторонний контроль безопасности вносит вклад в качество и безопасность продуктов и услуг организации. Это хорошо понимается как органами осуществляющими регулирование вопросов обеспечения безопасности, так и акционерами, клиентами, поставщиками оборудования и средств защиты. Таким образом, информирование заинтересованных сторон о наличии в организации систем периодического самоаудита способствует большему доверию к ней, к ее продукции услугам.

В качестве образца для построения отраслевых систем управления безопасностью на основании самооценки (самоаудита) безопасности может быть предложена хорошо продуманная система стандартов и рекомендаций обеспечения информационной безопасности организаций банковской системы Российской Федерации, разработанная в Банке России [1–5].

Однако нельзя не отметить, что реально проводить самоаудит без использования программных средств его поддерживающих невозможно. Все последние годы в Банке России для периодической ежеквартальной самооценки безопасности в региональных расчетных системах практически во всех регионах Российской Федерации используется программный комплекс «АванГард», разработанный в Институте системного анализа Российской академии наук (ИСА РАН), который дает возможность осуществлять контроль состояния безопасности КВО в масштабе всей страны [6–15].

В дальнейшем с учетом опыта разработки систем самооценки для ЦБ РФ в ИСА РАН был разработаны программные комплексы для аудита и самоаудита информационной безопасности критически важных объ-

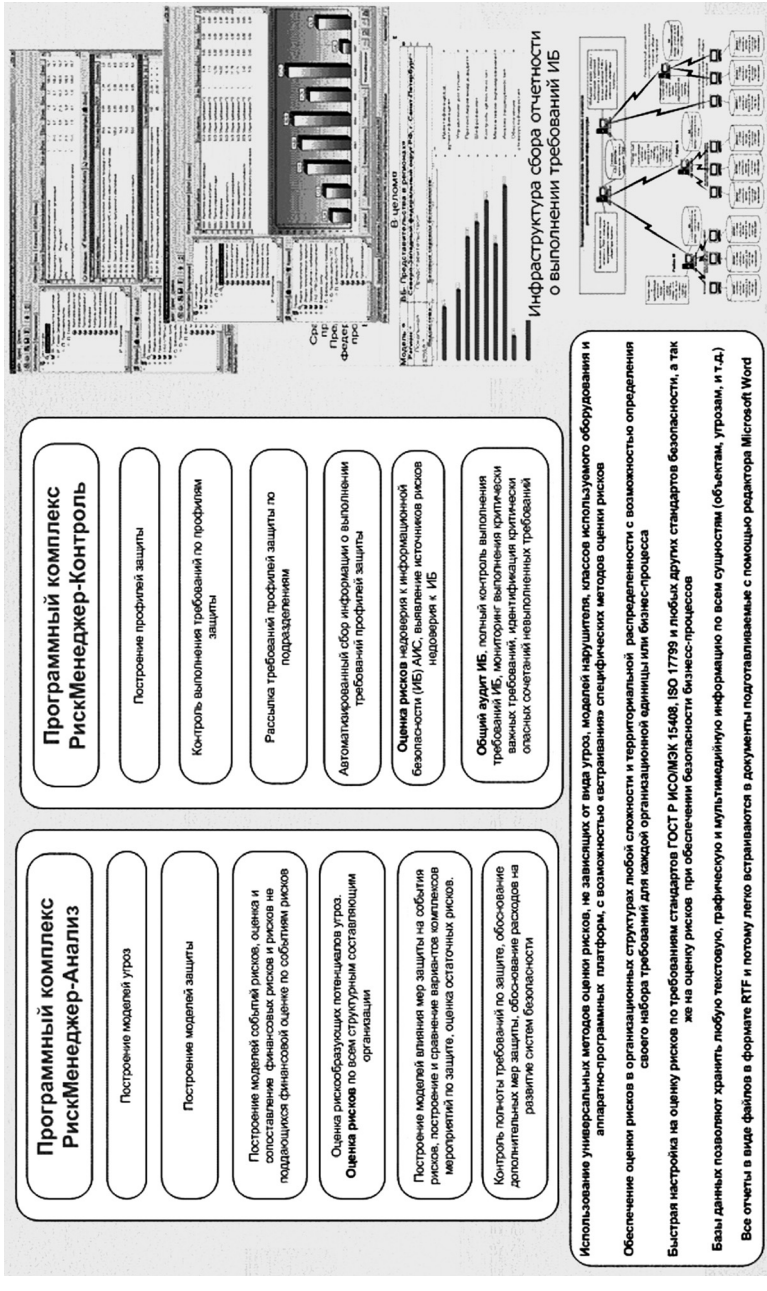

Рис. 1. Основные функциональные возможности программных комплексов «РискМенеджер-Анализ» и «РискМенеджер-Контроль»

ектов самых разных областей «РискМенеджер-Анализ» и «РискМенеджер-Контроль». Основные функциональные возможности этих комплексов представлены на рис. 1.

Фактически применение этих программных комплексов открывает возможности всестороннего глубокого контроля всей системы безопасности сколь сложна она бы не была.

Литература

1. Стандарт Банка России СТО БР ИББС–1.0–2006. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Принят и введен в действие Распоряжением Банка России 26 января 2006 г. № Р–27. М.: Банк России, 2006.
2. Стандарт Банка России СТО БР ИББС–1.1–2007. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». Принят и введен в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–345. М.: Банк России, 2007.
3. Стандарт Банка России СТО БР ИББС–1.2–2007. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС–1.0». Принят и введен в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–346. М.: Банк России, 2007.
4. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС–1.0» Приняты и введены в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–347. М.: Банк России, 2007.
5. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС–1.0». Приняты и введены в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–348. М.: Банк России, 2007.
6. *Владимирова Т. Н.* Опыт работы по внедрению системы мониторинга информационной безопасности платежной системы Банка России // Информационный бюллетень Главного управления безопасности и защиты информации Центрального банка Российской Федерации. 2005. № 1. С. 47–56.

7. *Бурдин О. А., Кононов А. А.* Метод оценки рискообразующих потенциалов в компьютеризированных организационных системах // НТИ. Сер. 1. 2004. № 2. С. 19–21.
8. *Кононов А. А.* Как обеспечить гарантированную безопасность информационной инфраструктуры // Информационное общество. 2005. № 2. С. 47–48.
9. *Кононов А. А., Поликарпов А. К.* Обеспечение безопасности информации: задачи и решения» // Информационная безопасность. 2005. № 5.
10. *Кононов А. А.* Оценка рисков доверия к кибербезопасности компьютеризированных систем // Проблемы кибербезопасности информационного общества: Труды Института системного анализа Российской академии наук. Т. 27. М.: КомКнига/URSS, 2006. С. 35–42.
11. *Кононов А. А., Поликарпов А. К.* Обеспечение гарантированной защиты информации в компьютерных системах // НТИ. Сер. 1. 2006. № 4. С. 42–43.
12. *Кононов А. А.* Оценка рисков доверия к безопасности автоматизированной информационной системы // НТИ. Сер. 2. 2006. № 10. С. 10–13.
13. *Kononov A. A.* An Estimation of the Risks of Confidence to the Safety of an Automated Information System // Automatic documentation and mathematical linguistics translations of selected articles from nauchno-tekhnicheskaia informatsiia. USA: Allerton Press Inc., 2006. Vol. 40. Part 5. P. 202–205.
14. *Черешкин Д. С., Кононов А. А., Сичкарук А. В.* Задачи управления киберрисками региональных критических инфраструктур // V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». Санкт-Петербург, 23–25 октября 2007 г. Материалы конференции. СПб., 2007. С. 17–18.
15. *Кононов А. А., Сичкарук А. В., Черныш К. В.* Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 31 М.: Издательство ЛКИ/URSS, 2007. С. 95–98.