ТЕОРИЯ И МЕТОДОЛОГИЯ УПРАВЛЕНИЯ

В.Л. Шульц, В.В. Кульба, А.Б. Шелков

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Аннотация. *Работа посвящена анализу технологий и разработке методов и моделей повышения эффективности аудита информационной безопасности автоматизированных систем. Приведены методы организации аудита рассматриваемого типа, анализ основных этапов аудита системы управления информационной безопасностью, включающих комплексное обследования системы, анализ существующих рисков и выработку рекомендаций по совершенствованию системы защиты информационных ресурсов. Поставлена и решена задача повышения эффективности организации проведения аудита информационной безопасности по критерию минимизации аудиторского риска. Процесс аудита представлен как совокупность взаимосвязанных по информации и времени аудиторских процедур. Для анализа и оценки аудиторского риска введено понятие "стандартной схемы обработки аудиторских данных", в рамках которого цикл обработки данных аудита распадается на непосредственно обработку, контроль и исправление ошибочных данных либо запрос дополнительной исходной информации, необходимой для реализации аудиторской процедуры. Методологическую основу исследования составляют системный, структурно-функциональный, сравнительный подходы, методы анализа, синтеза, индукции, дедукции, моделирования, наблюдения. Задача оптимизации процесса аудита состоит при этом в выборе такой технологии обработки аудиторских данных, которая обеспечивает максимум безошибочности получаемых результатов. Приведены модели и методика анализа эффективности, обоснования и выбора проектных решений по повышению уровня информационной безопасности из множества возможных альтернативных вариантов с использованием метода векторной стратификации.*

Ключевые слова: *информационная безопасность, автоматизированная система, аудит, аудиторский риск, стандартная схема, контроль, проектное решение, комплексная оценка, целенаправленный выбор, векторная стратификация.*

Введение

На современном этапе развития автоматизированных систем различного класса и назначения возрастает степень уязвимости перерабатываемой информации, что объясняется комплексом факторов, основными из которых являются: резкое увеличение объемов обрабатываемых данных; сосредоточение в единых базах данных большого объема информации различного назначения; развитие систем коллективного пользования, развитие автоматизированных систем на базе вычислительных сетей с высокой степенью автоматизации обмена информацией между ЭВМ[1] [2].

Основными принципиально возможными путями утечки информации при функционировании систем обработки данных являются: прямое хищение носителей информации и документов, используемых при функционировании автомати-

[1] Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. // Под ред. Н.А. Кузнецова, В.В. Кульбы. – М.: Наука 2006.

[2] Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. Издание второе. Серия «Информационные технологии». – М.: СИНТЕГ, 2003.

DOI: 10.7256/2307-9118.2014.4.10281

зированных систем; копирование информации, записанной на материальных носителях (машинных и немашинных); несанкционированное подключение к аппаратуре передачи данных (терминалу пользователей) и незаконное ее использование для доступа к информации; несанкционированный доступ к данным с помощью специально разработанных для этой цели программных средств; использование специальных технических средств для перехвата и расшифровки электромагнитных волн, излучаемых техническими средствами передачи и данных в процессе переработки информации.

В общеупотребительном смысле под информационной безопасностью автоматизированных систем понимается поддержание физической сохранности, доступности, конфиденциальности, достоверности и своевременности информации, а также гарантированной работоспособности средств, используемых для ввода, хранения, обработки и передачи данных. Более строгое определение дается в Руководящем документе Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», где информационная безопасность определяется как защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации или поддерживающей инфраструктуре[3].

Вопросы правового обеспечения деятельности в области защиты информации регулируются Федеральным законом от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации". В упомянутом Федеральном законе введена система понятий и определений, являющихся основополагающими при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Наиболее значимыми нормативными документами, определяющими критерии оценки уровня информационной безопасности и требования, предъявляемые к механизмам защиты, являются Руководящие документы Гостехкомиссии (в зарубежных странах аналогичные функции выполняют соответствующие национальные стандарты), «Общие критерии оценки безопасности информационных технологий» (The Common Criteria for Information Technology Security Evaluation/ISO 15408) и «Практические правила управления информационной безопасностью» (Code of practice for Information security management/ISO 17799) и др[4] [5].

1. Организация аудита систем обеспечения информационной безопасности

Целью проведения аудита является проверка соответствия выбранных организационных и технологических решений по обеспечению информационной безопасности определенным в политике безопасности автоматизированных систем требованиям и ограничениям. В процессе проведения аудита основное внимание обычно уделяется следующим основным вопросам[6] [7]:

- определение и обоснование границ проводимого аудита;
- выбор методики оценки системы управления информационной безопасностью;
- оценка степени соответствия существующего режима информационной безопасности требованиям организации и используемым стандартам, нормативам и регламентам;

[3] Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. - М.: ООО «ТИД «ДС»», 2001.

[4] Галатенко В. Стандарты информационной безопасности. - М.: Интуит.Ру, 2004.

[5] Павельев С.В. Методы и критерии комплексной оценки интегрального уровня безопасности информационных активов компании. // Труды XI Международной конференции по проблемам управления безопасностью сложных систем. Часть 1. - М.: ИПУ РАН, 2003..

[6] Астахов А. Анализ защищенности корпоративных систем. // Открытые системы, №07-08, 2002.

[7] Калашников А.О., Котухов М.М., Личманов И.А. Практические вопросы аудита состояния информационной безопасности корпоративных информационных систем. // Information Security, №3 2004.

DOI: 10.7256/2307-9118.2014.4.10281

- формулировка развернутой системы выводов и рекомендаций по совершенствованию системы управления информационной безопасностью.

Аудит системы управления информационной безопасностью осуществляется в три этапа:

- проведение комплексного обследования системы;
- проведение анализа существующих рисков;
- разработка рекомендаций по совершенствованию системы защиты информационных ресурсов и плана их практического внедрения.

Комплексное обследование проводится с целью сбора информации о существующем положении дел по обеспечению информационной безопасности для всех ключевых составляющих автоматизированной системы заказчика. Информация, получаемая при проведении обследования, позволяет выявить возможные слабые места в системе информационной безопасности, определить адекватность и эффективность используемых организационно-технических мер, применяемых для защиты ресурсов в автоматизированной системе.

На данном этапе уточняются цели и задачи аудита, а также состав рабочей группы, в которую должны входить сотрудники заказчика, которые обеспечивают представление всей необходимой информации, контролируют процессы проведения обследования, а также участвуют в согласовании его результатов. Представители от исполнителя в рабочей группе отвечают за квалифицированное проведение работ по обследованию предметных областей в соответствии с определенными целями и задачами проекта, согласуют процессы и результаты проведения обследования.

Основными задачами, решаемыми при проведении комплексного обследования, являются следующие:

- сбор и анализ документированной информации;
- анализ и изучение существующей организационно-штатной структуры заказчика, а также структуры и порядка функционирования автоматизированной системы;
- интервьюирование персонала;
- анализ конфигурации типовых рабочих мест, ключевых устройств и серверов.

На этапе комплексного обследования собранная информация систематизируется и анализируется на предмет непротиворечивости, полноты и достаточности. По результатам анализа определяются последующие действия - формирование запросов на получение дополнительной информации и проведение дополнительных исследований.

Существующая документированная информация о функционировании автоматизированной системы выборочно проверяется посредством интервью и в процессе анализа конфигурации сетевого оборудования и серверов. Существующие недокументированные процессы, существенные с точки зрения информационной безопасности, которые выявляются по результатам интервью и визуального наблюдения, документируются и включаются в отчет об обследовании.

Сбор и анализ информации с последующей ее оценкой, анализом рисков и выдачей рекомендаций осуществляется по следующим основным компонентам автоматизированной системы:

- топология автоматизированной системы и сетевые соединения;
- архитектура сопряжения с внешними информационными ресурсами и пользователями;
- типы информационных ресурсов на серверах заказчика;
- сведения о конфиденциальности и критичности данных;
- информационные потоки, циркулирующие в автоматизированной системе, характеристики передаваемой информации;
- системное программное обеспечение, организация и управление сетевыми сервисами;
- использование штатных средств операционных систем и сетевого оборудования;
- специализированные программно-технические средства защиты информации;
- существующие методы управления информационной безопасностью;
- концептуальные документы по информационной безопасности;
- специализированные средства защиты ресурсов автоматизированной системы;
- организационно-штатная структура подразделения, отвечающего за информационную безопасность;
- функции и зоны ответственности персонала;
- принципы и способы взаимодействия ответственного за обеспечение информационной безопасности подразделения с IT-подразделениями;

DOI: 10.7256/2307-9118.2014.4.10281

- иные организационные и технические меры и средства защиты информации.

Как уже было отмечено выше, информационной основой проводимых процедур сбора и анализа данных об обеспечиваемом уровне информационной безопасности является прежде всего существующая на момент обследования документированная информация. В ходе работ по аудиту производится сбор и анализ следующих форм документированной информации:

- проектная и эксплуатационная документация на автоматизированную систему;
- структурные и функциональные схемы участков автоматизированной системы;
- организационно-распорядительные и нормативно-технические документы по информационной безопасности;
- организационно-штатная структура подразделения, отвечающего за обеспечение информационной безопасности;
- перечень сведений конфиденциального характера;
- планы восстановления работоспособности автоматизированной системы при возникновении аварийных ситуаций;
- должностные инструкции персонала, ответственного за обеспечение информационной безопасности;
- программы и планы развития организационных и технических мер по обеспечению информационной безопасности.

Методы интервью и непосредственного наблюдения проводятся с целью получения исходной информации об автоматизированной системе и системе обеспечения информационной безопасности, отсутствующей в документированном виде, подтверждения актуальности документированной информации и определения уровня осведомленности сотрудников и персонала в части требований по обеспечению информационной безопасности.

Наблюдение за реальными процессами, связанными с обеспечением информационной безопасности, прежде всего осуществляется за функционированием следующих элементов и процессов автоматизированной системы:

- процедуры регистрации/исключения пользователей, генерации и смены паролей;
- процедуры анализа журналов аудита и реагирования на подозрительную активность;
- порядок изменения конфигурации и обновления системного программного обеспечения сетевых устройств и серверов;
- порядок обработки заявок на предоставление дополнительных прав доступа;
- порядок работы с комплексом средств защиты;
- действия, предпринятые при обработке произошедших инцидентов и в аварийных ситуациях;
- организация и регламентация доступа в серверные и иные технологические помещения;
- иные аспекты деятельности по обеспечению информационной безопасности.

При проведении анализа конфигурации типовых рабочих мест, сетевых устройств и ключевых серверов их перечень определяется по согласованию с руководством организации, осуществляющей эксплуатацию автоматизированной системы. Целью такого анализа является оценка соответствия реальной конфигурации тому, что определяется эксплуатационной документацией, требованиями политики безопасности и персоналом, а также определение существующих уязвимых мест автоматизированной системы. Наиболее важные и критичные с точки зрения обеспечиваемого уровня информационной безопасности аспекты конфигурации в обязательном порядке документируются и включаются в отчет об обследовании. Анализу подлежат прежде всего параметры аутентификации и контроля доступа, механизмы авторизации, доступа и управления, параметры аудита, меры защиты маршрутной информации, меры защиты от внешних атак и др.

Анализ рисков нарушения информационной безопасности позволяет идентифицировать существующие угрозы, оценить результаты их потенциального воздействия как на обследуемую автоматизированную систему, так и на деятельность организации - пользователя в целом.

Рассматриваемый этап является одной из важнейших стадий при аудите информационной безопасности. Анализ проводится для оценки (уточнения) реальных угроз нарушения информационной безопасности и разработки рекомендаций, выполнение которых позволит минимизировать эти угрозы и снизить ущербы от их реализации.

Анализ рисков дает возможность:

- адекватно оценить либо уточнить оценки существующих угроз и рисков;

DOI: 10.7256/2307-9118.2014.4.10281

- идентифицировать критичные ресурсы автоматизированной системы;
- выработать адекватные требования по защите информации;
- сформировать (уточнить) перечень наиболее опасных уязвимых мест, угроз и потенциальных злоумышленников;
- получить определенный уровень гарантий, основанный на объективном экспертном заключении.

При анализе рисков в процессе аудита осуществляется:

- классификация информационных ресурсов;
- формирование модели потенциального злоумышленника;
- анализ источников уязвимости;
- идентификация и оценка угроз нарушения информационной безопасности;
- количественная оценка рисков нарушения информационной безопасности.

В процессе анализа рисков проводится оценка критичности идентифицированных уязвимых мест и возможности их использования потенциальным злоумышленником для осуществления несанкционированных действий. В настоящее время анализ рисков наиболее часто основывается на международных стандартах информационной безопасности[8]. На основании информации, полученной в ходе обследования автоматизированной системы заказчика и результатов анализа рисков, разрабатываются рекомендации по совершенствованию системы защиты, применение которых позволит минимизировать риски.

При *выработке рекомендаций* анализируются следующие характеристики построения и функционирования автоматизированной системы:

Организационные характеристики:

- наличие, полнота и актуальность организационно-распорядительных и нормативно-технических документов;
- разделение зон ответственности персонала по обеспечению информационной безопасности и его корректность;
- наличие документированных списков, описывающих полномочия сотрудников по доступу к сетевым устройствам и серверам;
- наличие планов по поддержке квалификации персонала, ответственного за обеспечение информационной безопасности;
- осведомленность пользователей и персонала, поддерживающего функционирование автоматизированной системы о требованиях по обеспечению информационной безопасности;
- корректность процедуры управления изменениями и процедуры установления обновлений;
- порядок предоставления доступа к внутренним ресурсам информационных систем;
- наличие механизмов разграничения доступа к документации.

Организационно-технические характеристики:

- возможности использования найденных уязвимых мест для реализации удаленных атак;
- возможность оперативного анализа журналов аудита и реагирования на события, связанные с попытками несанкционированного доступа, оценка полноты анализируемых событий, оценка адекватности защиты журналов аудита;
- наличие процедур по обнаружению и фиксации инцидентов информационной безопасности и механизмов расследования таких инцидентов;
- уровень документирования любых действий, связанных с модификацией прав доступа, изменениями параметров аудита;
- периодичность контроля защищенности сетевых устройств и серверов;
- наличие процедуры отслеживания новых уязвимостей в системном программном обеспечении и его обновления;
- ограничение доступа в серверные помещения;
- адекватность времени восстановления в случае сбоев критичных устройств и серверов;
- наличие зоны опытной эксплуатации новых проектных решений, процедуры их тестирования и ввода в промышленную эксплуатацию.

Технические характеристики, связанные с архитектурой автоматизированной системы:

[8] Калашников А.О., Котухов М.М., Личманов И.А. Практические вопро-сы аудита состояния информационной безопасности корпоративных информационных систем. // Information Security, №3, 2004.

DOI: 10.7256/2307-9118.2014.4.10281

- топология и логическая организация сетевой инфраструктуры, адекватность контроля доступа, адекватность сегментирования;
- топология и логическая организация системы защиты периметра, адекватность контроля доступа из внешних сетей;
- топология, логическая организация и адекватность контроля логических путей доступа между сегментами;
- наличие узлов, сбои на которых приведут к невозможности функционирования значительной части (критически важной с точки зрения целей и задач) автоматизированной системы;
- наличие точек удаленного доступа к информационным ресурсам автоматизированной системы и адекватность защиты такого доступа.

Технические характеристики, связанные с конфигурацией сетевых устройств и серверов автоматизированной системы:

- права доступа персонала к сетевым устройствам и серверам, оценка минимально необходимых прав, которые требуются для выполнения производственных задач;
- соответствие списков контроля доступа на критичных сетевых устройствах документированным требованиям;
- соответствие конфигурации операционных систем и штатных механизмов информационной безопасности рекомендациям производителя и наилучшей практике;
- наличие неиспользованных сервисов или сервисов, содержащих известные уязвимости;
- соответствие механизма и стойкости процедуры аутентификации - критичности ресурсов, оценка адекватности парольной политики и протоколирования деятельности операторов.

Технические характеристики, связанные с использованием встроенных механизмов информационной безопасности:

- оценка соответствия конфигурации встроенных средств защиты документированным требованиям и оценка адекватности существующей конфигурации;
- оценка адекватности использования криптографической защиты информации и процедуры распределения ключевой информации;
- наличие антивирусной проверки трафика, а также антивирусного контроля на рабочих станциях пользователей;
- наличие резервных копий файлов конфигурации и образов дисков для критичных устройств и серверов;
- наличие источников бесперебойного питания для критичных сетевых устройств и серверов и их адекватность требованиям по времени бесперебойной работы.

Рекомендации по результатам аудита информационной безопасности включают предложения и рекомендации:

- по совершенствованию архитектуры и организации построения автоматизированной системы;
- по изменению конфигурации существующих сетевых устройств и серверов;
- по изменению конфигурации существующих средств защиты;
- по активации дополнительных штатных механизмов безопасности на уровне системного программного обеспечения;
- по использованию дополнительных средств защиты;
- по разработке организационно-распорядительных и нормативно-технических документов;
- по разработке программы осведомленности сотрудников в части информационной безопасности;
- по пересмотру ролевых функций персонала и зон ответственности;
- перечень мероприятий по поддержке и повышению квалификации персонала;
- периодичность и содержание работ по проведению анализа рисков и аудита по информационной безопасности;
- по этапам развития системы информационной безопасности заказчика.

При разработке рекомендаций в обязательном порядке делается ссылка на те уязвимые места, которые устраняются или минимизируются, а также на те риски, которые могут быть снижены за счет внедрения рекомендаций. Перечень рекомендаций согласуется с заказчиком на предмет возможности их реализации. Определяются рекомендации, которые могут быть реализованы заказчиком самостоятельно, и рекомендации, для реализации которых необходимо привлечение внешнего под-

DOI: 10.7256/2307-9118.2014.4.10281

рядчика. Совместно с заказчиком определяются этапы реализации рекомендаций и определяются точки и механизмы контроля. Следует подчеркнуть, что оценке и выдаче рекомендаций подлежит не только документированная деятельность по обеспечению информационной безопасности, но и деятельность, осуществляемая персоналом заказчика на недокументированной основе. В последнем случае в отчете об обследовании эксперты по сути производят документирование такой деятельности.

2. Методы анализа и синтеза технологий аудита по критерию минимизации аудиторского риска

На качество результатов аудита информационной безопасности автоматизированных систем значительное влияние оказывает аудиторский риск, анализ и оценка которого должна проводиться на этапе подготовки комплекса аудиторских процедур. Если данный риск превышает допустимые пределы, необходима разработка или корректировка плана работ для его снижения до приемлемо низкого (допустимого) уровня.

Под *аудиторским риском* (по аналогии с аудитом экономических субъектов[9] [10]) будем понимать вероятность формирования неверного вывода, и, как следствие, выработку неверных рекомендаций в процессе проведения аудита информационной безопасности.

Основными процедурами аудита информационной безопасности, как было указано выше, являются комплексное обследование автоматизированной системы, анализ технической документации, текущей документированной информации, накопленной статистики о функционировании системы, системных и регистрационных журналов, конфигурации типовых рабочих мест, ключевых устройств и серверов, необходимых данных из иных внешних и внутренних источников, интервьюирование персонала, оценка степени соответствия принятых мер безопасности действующим нормативным документам и техническим регламентам, оценка рисков и прогнозирование величины возможных ущербов, формирование и обоснование технических предложений по обеспечению заданного уровня информационной безопасности. Длительность выполнения указанных процедур зависит помимо трудоемкости от срока, отведенного на получение аудиторских доказательств и представления технических предложений заказчику[11].

По своей сути рассматриваемый тип аудита во многом аналогичен этапам предпроектного анализа и технического проектирования автоматизированной системы и связан с аналитической обработкой достаточно большого объема качественных и количественных данных. При этом аудиторские процедуры могут быть ручными, автоматизированными и автоматическими. При этом в процессе аудита приходится решать аналитические, расчетные и информационные задачи (а в ряде случаев и оптимизационные).

На первом этапе (этап анализа) аудит информационной безопасности представляет собой проверку документальной информации, результатом которой являются так называемые аудиторские доказательства различной степени надежности и достоверности (в зависимости от их характера и источника, а также процедур обработки), которые, по сути, являются обоснованием для последующей выработки технических предложений по обеспечению заданного уровня информационной безопасности. При этом документальные аудиторские доказательства, включают в себя:

- документальные аудиторские доказательства, созданные третьими лицами (внешняя информация);
- документальные аудиторские доказательства, созданные третьими лицами, но находящиеся на объекте аудита (внешняя и внутренняя информация);
- документальные аудиторские доказательства, созданные на объекте аудита (внутренняя информация).

В принципе аудит представляет собой совокупность специальных приемов (методов), используемых для обработки исходной информации для достижения поставленных целей. Многообразные приемы аудита обычно объединяют в четыре группы: определение реального состояния объ-

[9] Шеремет А.Д., Суйц В.П. Аудит. – М.: Инфра-М, 2005.

[10] Гладков Ю.М., Микрин Е.А., Шелков А.Б. Анализ и синтез механизмов минимизации аудиторского риска // Проблемы управления, № 2, 2007.

[11] Шеремет А.Д., Суйц В.П. Аудит. – М.: Инфра-М, 2005.

DOI: 10.7256/2307-9118.2014.4.10281

ектов, анализ, оценка, формирование технических предложений.

Пусть правильность или безошибочность результатов каждой аудиторской процедуры осуществляется с использованием принципа обратной связи. Тогда задача оптимизации технологии аудита (обработки аудиторских данных) состоит в выборе такой технологии обработки (т.е. определение процедур обработки, этапов контроля и исправления обнаруженных аудиторских ошибок, выбор методов обнаружения и исправления ошибок), которая обеспечивает минимизацию уровня аудиторского риска или максимизацию вероятности формирования безошибочных выводов по результатам аудита при заданных ограничениях на время и материальные затраты. Возможна постановка обратной задачи – выбор оптимальной технологии обработки данных в процессе аудиторских процедур, минимизирующей время и материальные затраты при ограничении на безошибочность результатов аудита.

Для анализа и оценки аудиторского риска введем понятие "стандартной схемы обработки аудиторских данных" (рис. 1). Цикл обработки данных аудита распадается на непосредственно обработку, контроль и исправление ошибочных данных либо запрос дополнительной исходной информации, необходимой для реализации аудиторской процедуры (далее для краткости – фаза исправления ошибок). На некоторых этапах обработки операции контроля и исправления недостоверных данных могут отсутствовать, либо могут осуществляться в несколько этапов, на каждом из которых, в свою очередь, осуществляется локальный контроль и исправление ошибок. После исправления ошибочных аудиторских данных они вновь обрабатываются с последующим контролем и исправлением. Контроль и исправление могут повторяться случайное число раз. Производными стандартной схемы обработки данных являются последовательная схема обработки, последовательная схема с общей обратной связью, циклическая и последовательно – циклическая схема, сеть обработки данных[12].

Пусть процесс обработки единицы входных данных является процессом Бернулли, в котором q – вероятность возникновения ошибки при обработке единичного объема данных, а вероятность правильной обработки единичного объема $p=1–q$.

Процесс контроля также является бернуллиевским, где f – вероятность обнаружения ошибки в единичном объеме данных и $e=1–f$ – вероятность пропуска ошибки. Предполагается, что вероятность принятия правильно обработанного единичного объема данных за ошибку равна нулю. Обнаруженные ошибки исправляются с вероятностью, равной единице.

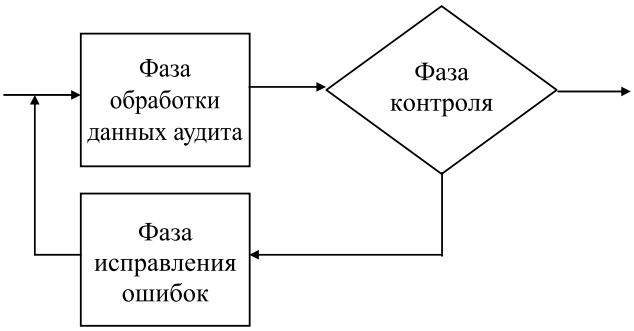

Рис. 1. Стандартная схема обработки данных

Под единицей объема данных в зависимости от задачи или этапа процесса аудита понимается число, запись, сообщение, массив, документ и т.д., а N – общий объем данных.

Число циклов обработки единицы данных является случайным и попытка обработки считается успешной, если в фазе обработки не произошло ошибки или же ошибка произошла, но не была обнаружена в фазе контроля. Попытка считается неуспешной, если в фазе обработки произошла ошибка, которая не была обнаружена.

Обозначим через ξ_k число попыток, затрачиваемых в фазе обработки на k-ю единицу данных, $k=\overline{1,N}$. Тогда число попыток $T(N)$, затрачиваемых в фазе обработки на единицу данных, равно сумме случайных величин ξ_k. Если на реализацию попытки в фазе обработки требуется единичное время, то $T(N)$ – время, затраченное на обработку N единиц данных.

Основной задачей анализа рассматриваемой схемы является нахождение закона распределения $\Phi(N,x)=P\{T(N)\le x\}$ случайной величины $T(N)$. Задачи, связанные с определением вероятностных характеристик времени, которое тратится на об-

[12] Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. // Под ред. Н.А. Кузнецова, В.В. Кульбы. – М.: Наука, 2006.

DOI: 10.7256/2307-9118.2014.4.10281

работку данных объема N в фазах обнаружения и исправления, решаются аналогично.

Рассмотрим случай, когда ошибки при обработке данных (реализации аудиторских процедур) возникают независимо. Процесс обработки единицы данных может завершиться успехом на ($k+1$)-й попытке, если данные не содержат ошибок с вероятностью $(qf)^k p$, либо если данные с вероятностью $(qf)^k q(1-f)$ содержат необнаруженные ошибки. В противном случае процесс обработки рассматриваемых данных единичного объема не заканчивается и они должны быть обработаны, по крайней мере, еще один раз. Вероятность этого события равна $(qf)^{k+1}$, и случайные величины ξ_k имеют геометрическое распределение, т.е.

$$P\{\xi_k = i\} = (qf)^{i-1}(p+qe),$$

где $i \geq 1$. Вероятность того, что за время i данные единичного объема будут обработаны без ошибок, определяется как

$$P_1(i) = \sum_{j=0}^{i-1} p(qf)^j.$$

Представив $P_1(i)$ в виде $P_1(i) = \rho\rho_1\rho_2$, где $\rho_1 = (1-qf)^{-1}$ и $\rho_2 = l_2 - (qf)^i$; получим, что при $i \to \infty$ вероятность безошибочной обработки данных единичного объема равна $\rho\rho_1$, и $\lim\limits_{i\to\infty} P_1(i) = 1$ только при $f = 1$. Вероятность того, что за время $(i-1)$ произошла обработка $(N-1)$-й единицы данных и было $(i-N)$ неудачных попыток обработки, равна $C_{i-1}^{N-1}(p+qe)^{N-1}(qf)^{i-N}$.

Вероятность удачной попытки равна $p+qe$, поэтому закон распределения времени обработки данных объемом N имеет вид:

$$P\{T(N) = i\} = \begin{cases} 0, \text{ при } i \leq N, \\ C_{i-1}^{N-1}(p+qe)^N (qf)^{i-N}, \ i \geq N. \end{cases} \quad (1)$$

Математическое ожидание и дисперсия случайной величины $T(N)$, распределенной по отрицательному биномиальному закону (1), определяется, соответственно, как

$$M[T(N)] = N(1-qf)^{-1}, \ D[T(N)] = Nqf(1-qf)^{-2}.$$

Использование эффективных методов контроля ($f \to 1$) увеличивает $M[T(N)]$, а при $f \to 0$, $M[T(N)] \to N$. Если N велико, то на основании центральной предельной теоремы величина $T(N)$, как сумма независимых одинаково распределенных случайных величин ξ_k, распределена по нормальному закону:

$$\Phi(N,x) = P\{T(N) \leq x\} \approx \Phi^*\left(\frac{(1-qf)x - N}{\sqrt{Nqf}}\right),$$

где $\Phi^*(Z) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{Z} e^{t^2/2} dt.$

Полученные результаты являются основой решения задач о выделении необходимых временных и стоимостных ресурсов на обработку данных заданного объема. Для того чтобы с доверительной вероятностью, не меньшей α, были обработаны данные объема N, выделяемое с этой целью время $\overline{T}$ должно быть определено из условия

$$\Phi^*\left[\frac{(1-qf)\overline{T} - N}{\sqrt{Nqf}}\right] \geq \alpha.$$

Пусть t_α – такое значение квантили нормального закона распределения, что $\Phi^*(t_\alpha) = \alpha$. Так как $\Phi^*(Z)$ – монотонно возрастающая функция, условие реализуемости обработки данных аудита объема N запишется в виде:

$$\overline{T} \geq \left(N + t_\alpha\sqrt{Nqf}\right)(1-qf)^{-1}. \quad (2)$$

Соответствующее условие для стоимостного ресурса $\overline{C}$ записывается аналогично.

Полученные результаты сведены в табл. 1.

Таблица 1

Характеристики методов обработки и контроля данных аудита

Характеристики процесса обработки аудиторских данных	Расчетные выражения
Математическое ожидание $M[T(N)]$	$\frac{N}{(1+qf)}$
Дисперсия $D[T(N)]$	$\frac{Nqf}{(1-qf)^2}$
Вероятность $P\{T(N) = k\}$ для небольших N, $k \geq N$	$\binom{N-1}{k-1}(1-qf)^N (qf)^{k-N}$
Непрерывный аналог функций распределения $\Phi(N,x)$	$\Phi^*\left(\frac{(1-qf)x - N}{\sqrt{Nqf}}\right)$

DOI: 10.7256/2307-9118.2014.4.10281

Характеристики процесса обработки аудиторских данных	Расчетные выражения
Необходимый временной ресурс T для обработки N единиц данных с доверительной вероятностью a	$\overline{T} \geq \frac{N + t_a\sqrt{Nqf}}{1-qf}$
Необходимый стоимостной ресурс $\overline{C}$ для обработки N единиц данных с доверительной вероятностью a	$\overline{C} \geq C\frac{N + t_a\sqrt{Nqf}}{1-qf}$

Полученные соотношения, устанавливающие взаимосвязь между характеристиками методов контроля и обработки аудиторской информации и требуемыми временными и стоимостными ресурсами, являются основой для решения задач выбора оптимальных методов контроля при реализации аудиторских процедур.

Предложенная формализованная методология охватывает достаточно широкий класс задач, возникающих при планировании и реализации аудиторских процедур различного типа и позволяет проводить анализ и оценку возникающих при этом аудиторских рисков.

3. Анализ эффективности проектных решений по обеспечению информационной безопасности

Одной из ключевых особенностей аудита рассматриваемого типа является наличие наиболее ответственного, завершающего этапа - формирования и обоснования технических предложений по обеспечению заданного уровня информационной безопасности. По сути, аудиторы должны предложить одно из типовых проектно – технических решений, обеспечивающих достижение поставленных целей.

Как известно, в настоящее время затраты на обеспечение информационной безопасности составляют значительную долю ресурсов многих организаций, в силу чего важное значение приобретает проблема анализа и оценки эффективности капитальных и текущих затрат на указанные цели.

Одним из основных подходов, применяемых в настоящее время для оптимизации затрат на проектирование, внедрение или приобретение различных систем и средств безопасности, является анализ и управление рисками[13][14]. Как уже было отмечено выше, в теории рисков и безопасности выделяют следующие объекты исследования:

- источники угроз (опасности) информационной безопасности;
- защищаемые ресурсы (объекты риска или безопасности);
- связи между источниками угроз и защищаемыми ресурсами;
- системы защиты ресурсов автоматизированных систем, создаваемые субъектами обеспечения информационной безопасности.

Простейшей мерой риска является пара: оценки вероятности Q неблагоприятного события и ущерба W при его наступлении. Оба показателя могут быть мультипликативным образом объединены в один: $R = Q \bullet W$, что позволяет сравнивать ситуации с различными последствиями и вероятностями их наступления.

Анализ эффективности принимаемых проектных решений по обеспечению информационной безопасности автоматизированных систем требует всесторонней комплексной оценки альтернативных вариантов, в основе которой лежит комплексный анализ риска. При этом в качестве основных критериев выступают следующие показатели:

- возможный ущерб от нарушения нормальной работы автоматизированной системы в результате сбоев и отказов в результате реализации угроз;
- вероятность наступления нежелательных событий, наносящих существенный ущерб;
- затраты (капитальные и эксплуатационные) на мероприятия по обеспечению требуемого уровня информационной безопасности.

Поэтому актуальной является задача выбора методики анализа, обоснования и выбора оптимальной системы защиты ресурсов автоматизированной системы из множества возможных альтернативных решений. Данная задача обычно решается на завершающем и наиболее важном этапе аудита информационной безопасности, основной целью которого является выработка рекомендаций по снижению внешних и внутренних рисков (и, соответственно, ущербов).

[13] Управление рисками: обзор употребительных подходов. Часть I. // «Jet Info», №11 (162), 2006.

[14] Управление рисками: обзор употребительных подходов. Часть II // «Jet Info», №12 (163), 2006.

DOI: 10.7256/2307-9118.2014.4.10281

Используемые модели выбора включают принцип выбора и множество выбора. Типичная модель задачи принятия решений имеет следующий вид[15] [16] [17] [18]:

$$M = < T, S, K, X, F, P, R >,$$

где T – постановка (тип) задачи; S – множество вариантов возможных решений; K – множество показателей и их весовых коэффициентов; X – множество шкал показателей; F – отображение множества допустимых решений во множество векторных оценок; P – система предпочтений лица, принимающего решения; R – решающее правило.

Знание целевой функции и весовых коэффициентов показателей в значительной степени снимает неопределенность данной задачи принятия решений.

Под весовыми коэффициентами показателей понимается нормированное приращение целевой функции, приходящееся на единицу приращения одного показателя, инвариантное относительно фиксированных уровней значений по остальным показателям. Большинством разработчиков методик комплексного оценивания, использующих метод линейной свертки частных показателей, данное требование инвариантности считается автоматически выполняющимся при любых условиях. В действительности, в задачах, имеющих практический смысл, приращение целевой функции, приходящееся на единицу приращения одного показателя, обычно зависит от того, на каком уровне зафиксированы значения по остальным показателям. Таким образом, значения весовых коэффициентов показателей, как правило, будут меняться в зависимости от того, на каких участках шкал производится их соизмерение. Кроме того, линейная монотонная функция свертки требует допустимости взаимной компенсации худших оценок по одним показателям лучшими оценками по другим показателям, что на практике далеко не всегда возможно.

В настоящее время в литературе практически отсутствуют рекомендации по построению формализованных процедур структуризации декларированных целей и формированию системы показателей. Значительное число публикаций содержит подходы к декомпозиции целей, но даже в наиболее известных и широко применяемых, например, в методе «ПАТТЕРН» и методе анализа иерархий Т. Саати[19] [20], не приведены хотя бы частично формализованные процедуры формирования системы показателей. Исключение представляют работы, использующие последовательную дихотомию, как регулярную процедуру декомпозиции заданной формулировки цели, для построения бинарной структуры показателей[21] [22]. Таким образом, в большинстве публикаций по теории принятия решений методологически наименее обеспечен этап формирования системы показателей. Если же выбранная система показателей неадекватна заданной цели, то никакие усилия при построении решающих правил, включая определение относительной важности показателей, не смогут компенсировать данного упущения. Экспертам очень трудно корректно определить вклад отдельных показателей при большом их числе. Кроме того, коэффициенты относительной важности могут изменяться при сопоставлении важности значений показателей на различных участках их шкал.

Перечисленные недостатки широко применяемых методик, использующих линейные свертки оценок по показателям, приводят к необходимости применения иных методов решения поставленных задач выбора. Методика целенаправленного выбора и метод векторной стратификации для

[15] Саати Т. Принятие решений. Метод анализа иерархий. - М.: Радио и связь, 1993.

[16] Macecrimmon K.P. Improving the system design and evaluation process by the use of trade of information: an application fourth last corridor transporta-tion planning RM 5877 – Dot // The Rand corporation. Cal.: Santa Monica. 1969.

[17] Айзерман М.А., Малишевский А.В. Проблемы логического обоснова-ния в общей теории выбора. Общая теория выбора и его классическо-рациональное основание. – М.: ИПУ РАН, 1980.

[18] Подиновский В.В., Ногин В Д. Парето-оптимальные решения многокритериальных задач. – М.: Наука, 1992.

[19] Айзерман М.А., Малишевский А.В. Проблемы логического обоснования в общей теории выбора. Общая теория выбора и его классическо-рациональное основание. – М.: ИПУ РАН, 1980.

[20] Лопухин М.М. ПАТТЕРН-метод планирования и прогнозирования научных работ. – М.: Сов. Радио. 1981.

[21] Глотов В.А., Павельев В.В. Векторная стратификация. – М.: Наука. 1984

[22] Павельев В.В. Формирование системы критериальных свойств при комплексной оценке сложных объектов / В кн.: Механизмы функционирования организационных систем. Вып. 29. – М.: ИПУ РАН, 1982.

DOI: 10.7256/2307-9118.2014.4.10281

построения системы показателей и соизмерения их важности при вычислении комплексной оценки, позволяют преодолеть перечисленные трудности. Метод векторной стратификации в процессе своего многолетнего использования при решении самых различных задач оценивания, выбора и принятия решений показал высокую эффективность, а также ряд преимуществ по сравнению с методами аналогичного назначения. В основе методики целенаправленного выбора лежит следующий принцип: комплексное оценивание должно обеспечивать измерение степени соответствия объекта оценки сформулированному целевому назначению.

Основные данные о рассматриваемом объекте оценки, в соответствии с методикой, структурируются в виде бинарного дерева характеристик объекта и оцениваются экспертами в балльных шкалах. С помощью решающего правила, которое отражает техническую и экономическую политику организации и представляет собой структурированную совокупность матриц логической свертки частных оценок, формируется комплексная оценка предлагаемого варианта в балльной шкале.

Принцип построения фрагмента древовидной структуры показателей путем их дихотомической детализации показан на рис. 2.

Рис. 2. Древовидная структура проекта

Алгоритм комплексной оценки представлен на рис.3.

Значения первичных показателей представляются в числовом и в качественном (словесном) выражении (например, оценка – высокая, средняя, низкая). Значения показателей преобразуются в единую шкалу из пяти градаций:

5-я страта – очень высокое значение показателя,

4-я страта – высокое значение показателя,

3-я страта – среднее значение показателя,

2-я страта – низкое значение показателя,

1-я страта – очень низкое значение показателя.

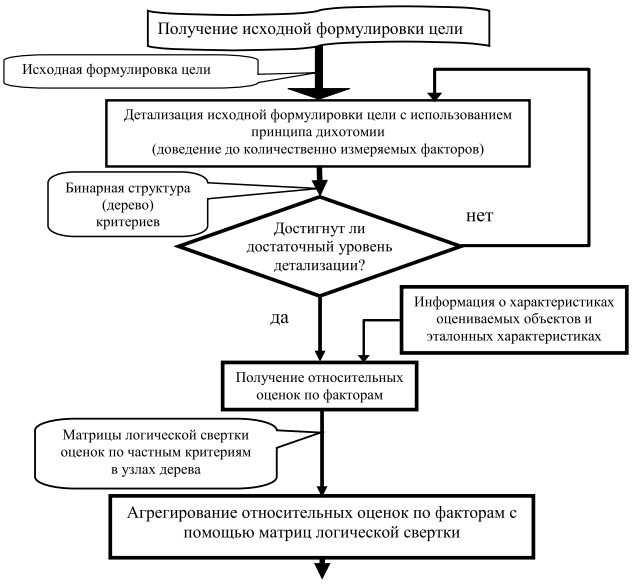

Рис. 3. Алгоритм комплексной оценки проекта

Числовые показатели нормируются относительно наилучшего (эталонного) значения так, чтобы наилучшее нормированное значение было максимальным и равным единице. Если наилучшим значением показателя является его максимальное значение, то при нормировании используется именно оно. Если же наилучшим значением показателя по смыслу является его минимальное значение, то при нормировании значение показателя заменяется его обратной величиной. Перевод нормированных числовых значений показателей в шкалу стратификации (или упорядоченной классификации) из пяти градаций и далее в пятибалльную шкалу производим с помощью психофизической шкалы Харрингтона[23] [24] [25], имеющей следующий вид:

[23] Глотов В.А., Павельев В.В. Векторная стратификация. – М.: Наука. 1984.

[24] Павельев В.В. Формирование системы критериальных свойств при комплексной оценке сложных объектов / В кн.: Механизмы функционирования организационных систем. Вып. 29. – М.: ИПУ РАН, 1982.

[25] Левинталь А.Б. и др. Комплексное оценивание и планирование развития региона. – М.: 2006.

DOI: 10.7256/2307-9118.2014.4.10281

5-я страта – очень высокое значение показателя *X*:

$0{,}8 < X \le 1 \Leftrightarrow$ 5 баллов;

4-я страта – высокое значение показателя *X*:

$0{,}63 < X \le 0{,}8 \Leftrightarrow$ 4 балла;

3-я страта – среднее значение показателя *X*:

$0{,}37 < X \le 0{,}63 \Leftrightarrow$ 3 балла;

2-я страта – низкое значение показателя *X*:

$0{,}2 < X \le 0{,}37 \Leftrightarrow$ 2 балла;

1-я страта – очень низкое значение показателя *X*:

$0 < X \le 0{,}2 \Leftrightarrow$ 1 балл.

Для каждого узла древовидной структуры показателей лицо, принимающее решение, или эксперты заполняют матрицы размерности 5×5 логической свертки частных оценок в баллах в обобщающую оценку. Строки матрицы соответствуют значениям оценок по одному из объединяемых показателей, столбцы – значениям оценок по второму показателю. Значения оценок варианта по обобщающему показателю проставляются на пересечении столбцов и строк. Их определяет эксперт или лицо, принимающее решение, с учетом относительной значимости объединяемых показателей.

При оценивании показателей обычно располагают сравнительно грубой информацией об относительной значимости вклада рассматриваемых оценок по обобщаемым показателям в комплексную оценку, например: «оценки равноценны», «оценка по показателю *X* важнее оценки по показателю *Y*», «оценка по показателю *X* гораздо важнее оценки по показателю *Y*». Заполненные матрицы логической свертки показателей, помещенные в соответствующих узлах древовидной структуры комплексного критерия, порождают решающее правило комплексной оценки. Оно может быть реализовано в виде компьютерной программы. Пример фрагмента такого правила представлен на рис. 4.

С помощью этого решающего правила все оцениваемые объекты можно разделить на 5 страт, упорядоченных по их предпочтительности. Самые лучшие отнесены к 5-й страте, самые худшие – к 1-й страте. Если в 5-й страте окажется несколько объектов оценки, то лучший из них выбирается с помощью дополнительной информации об условиях их применения.

В процессе комплексного оценивания сложного объекта можно провести анализ «узких мест» на дереве показателей. Такой анализ позволяет выявить причины появления нежелательно низких оценок

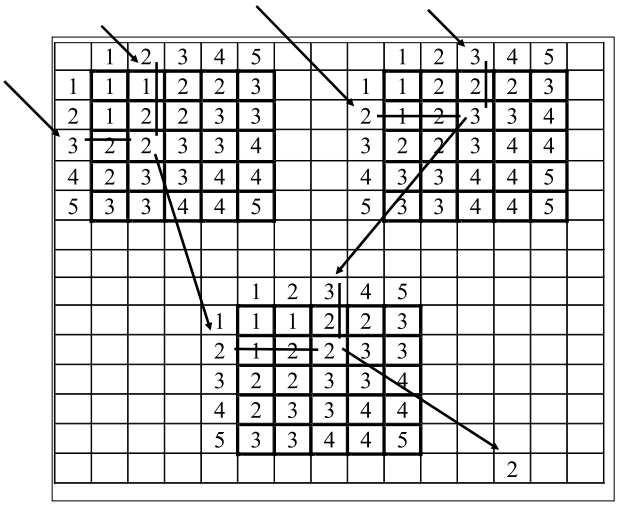

Рис. 4. Фрагмент алгоритма заполненные матрицы логической свертки показателей

показателей разного уровня обобщения и повысить значения комплексных оценок путем эффективного перераспределения ресурса между элементами рассматриваемого объекта. Процедура улучшения комплексной оценки объекта, как правило, носит интерактивный характер, поскольку каждое изменение локальных оценок требует интерпретации в терминах предметной области.

Понятие «узкого места» связано с понятием «сбалансированности» многокритериальной системы оценок. Для получения сбалансированной системы оценок необходимо, чтобы отсутствовали пары локальных критериев, входящих в одну свертку с резко различающимися значениями оценок. При построении сбалансированного дерева оценок каждая бинарная свертка должна быть по возможности симметричной по отношению к своим входам.

Если оценки объекта по сворачиваемым показателям имеют соседние значения по шкале баллов, например, по одному, более важному, – 4, а по другому, менее важному, – 5, и для оценки объекта используются *только целочисленные значения баллов*, то оценка по обобщающему показателю (результат свертки) будет равна оценке объекта по более важному показателю, т.е. 4 баллам. Если для большей точности используются и дробные значения оценок, то в данном случае результатом свертки будет соответствующее промежуточное значение, зависящее от относительной важности оценок объединяемых показателей.

DOI: 10.7256/2307-9118.2014.4.10281

Используемый подход[26] [27] дал возможность разработать методику, имеющую следующие свойства.

- Система критериев комплексной оценки формируется в процессе последовательной конкретизации цели и уточнения имеющихся знаний о предметной области.
- Формализация процедур комплексного оценивания использует аппарат бинарных деревьев и логических матриц свертки оценок по локальным критериям.
- Можно использовать как количественные (числовые), так и качественные (представленные словесными формулировками) исходные данные.
- Использование матриц логической свертки позволяет учесть изменение относительной важности рассматриваемых оценок по обобщаемым показателям в зависимости от того, на каких участках шкал производится их сравнение.
- При логической свертке оценок по парам показателей появляется возможность учитывать как допустимость, так и недопустимость взаимной компенсации худших оценок по одним показателям лучшими оценками по другим показателям (допустимости полной взаимной компенсации соответствует линейная монотонная функция свертки; абсолютной недопустимости взаимной компенсации соответствует функция *min(y1, y2)*; все остальные допустимые функции свертки также монотонны и находятся в диапазоне между этими крайними случаями).
- Используемые алгоритмы обобщения оценок по частным критериям отличаются простотой и наглядностью для лиц, принимающих решения.
- Предлагаемая методика позволяет увязать методы экспертного оценивания с математическим моделированием рассматриваемых объектов и процессов. Благодаря этому появляется возможность получать эффективные решения и, соответственно, вырабатывать рекомендации при рациональном сочетании результатов комплексного обследования автоматизированной системы и мнений экспертов (аудиторов).

Заключение

В работе получены следующие основные результаты:

Проведен анализ методов и основных этапов проведения аудита систем обеспечения информационной безопасности. Приведена классификация основных компонентов автоматизированной системы, детальный анализ функционирования которых проводится в процесса аудита. Сформулированы требования к процедурам анализа рисков и формирования рекомендаций по повышению уровня информационной безопасности.

Поставлена и решена задача повышения эффективности организации проведения аудита информационной безопасности по критерию минимизации аудиторского риска, анализ или оценка которого должна проводиться на этапе подготовки аудиторских процедур. Разработана формализованная модель оценки аудиторского риска. Процесс аудита представлен как совокупность взаимосвязанных по информации и времени аудиторских процедур. Для анализа и оценки аудиторского риска введено понятие "стандартной схемы обработки аудиторских данных", в рамках которого цикл обработки данных аудита распадается на непосредственно обработку, контроль и исправление ошибочных данных либо запрос дополнительной исходной информации, необходимой для реализации аудиторской процедуры. Задача оптимизации состоит при этом в выборе такой технологии обработки аудиторских данных, которая обеспечивает максимум их безошибочности. Возможна постановка обратной задачи – выбора оптимальной технологии обработки аудиторских данных, минимизирующей время и материальные затраты при ограничении на уровень аудиторского риска.

Разработаны модели и методика анализа эффективности, обоснования и выбора проектных решений по обеспечению заданного уровня информационной безопасности из множества возможных альтернативных решений с использованием метода векторной стратификации. Данная задача обычно решается на завершающем и наиболее важном этапе аудита информационной безопасности, основной целью которого является выработка рекомендаций по снижению внешних и внутренних рисков (и, соответственно, ущербов).

[26] Управление рисками: обзор употребительных подходов. Часть I. // «Jet Info», №11 (162), 2006.

[27] Управление рисками: обзор употребительных подходов. Часть II. // «Jet Info», №12 (163), 2006.

DOI: 10.7256/2307-9118.2014.4.10281

Библиография

1. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. // Под ред. Н.А. Кузнецова, В.В. Кульбы. – М.: Наука 2006.
2. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. Издание второе. Серия «Информационные технологии». – М.: СИНТЕГ, 2003.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-М.: ООО «ТИД «ДС»», 2002.
4. Галатенко В. Стандарты информационной безопасности.-М.: Интуит.Ру, 2004.
5. Павельев С.В. Методы и критерии комплексной оценки интегрального уровня безопасности информационных активов компании. // Труды XI Международной конференции по проблемам управления безопасностью сложных систем. Часть 1.-М.: ИПУ РАН, 2003.
6. Астахов А. Анализ защищенности корпоративных систем. // Открытые системы, №07-08, 2002.
7. Калашников А.О., Котухов М.М., Личманов И.А. Практические вопросы аудита состояния информационной безопасности корпоративных информационных систем. // Information Security, №3, 2004.
8. Шеремет А.Д., Суйц В.П. Аудит. – М.: Инфра-М, 2005.
9. Гладков Ю.М., Микрин Е.А., Шелков А.Б. Анализ и синтез механизмов минимизации аудиторского риска // Проблемы управления, №2, 2007.
10. Управление рисками: обзор употребительных подходов. Часть I. // «Jet Info», №11 (162), 2006.
11. Управление рисками: обзор употребительных подходов. Часть II // «Jet Info», №12 (163), 2006.
12. Саати Т. Принятие решений. Метод анализа иерархий.-М.: Радио и связь. 1993.
13. Macecrimmon K.P. Improving the system design and evaluation process by the use of trade of information: an application fourth last corridor transporta-tion planning RM 5877 – Dot // The Rand corporation. Cal.: Santa Monica. 1969.
14. Айзерман М.А., Малишевский А.В. Проблемы логического обоснования в общей теории выбора. Общая теория выбора и его классическо-рациональное основание. – М.: ИПУ РАН, 1980.
15. Подиновский В.В., Ногин В Д. Парето-оптимальные решения многокритериальных задач. – М.: Наука, 1992.
16. Лопухин М.М. ПАТТЕРН-метод планирования и прогнозирования научных работ. – М.: Сов. Радио, 1981.
17. Глотов В.А., Павельев В.В. Векторная стратификация. – М.: Наука, 1984.
18. Павельев В.В. Формирование системы критериальных свойств при комплексной оценке сложных объектов / В кн.: Механизмы функционирования организационных систем. Вып. 29. – М.: ИПУ РАН, 1982.
19. Левинталь А.Б. и др. Комплексное оценивание и планирование развития региона. – М.: 2006.

References (transliterated)

1. Informatsionnaya bezopasnost' sistem organizatsionnogo upravleniya. Teoreticheskie osnovy: v 2 t. // pod red. N.A. Kuznetsova, V.V. Kul'by. – M.: Nauka 2006.
2. Kul'ba V.V., Kovalevskii S.S., Shelkov A.B. Dostovernost' i sokhrannost' informatsii v ASU. Izdanie vtoroe. Seriya «Informatsionnye tekhnologii». – M.: SINTEG, 2003.
3. Domarev V.V. Bezopasnost' informatsionnykh tekhnologii. Metodologiya sozdaniya sistem zashchity.-M.: OOO «TID «DS»», 2002.
4. Galatenko V. Standarty informatsionnoi bezopasnosti.-M.: Intuit.Ru, 2004.
5. Pavel'ev S.V. Metody i kriterii kompleksnoi otsenki integral'nogo urovnya bezopasnosti informatsionnykh aktivov kompanii. // Trudy XI Mezhdunarodnoi konferentsii po problemam upravleniya bezopasnost'yu slozhnykh sistem. Chast' 1.-M.: IPU RAN, 2003.
6. Astakhov A. Analiz zashchishchennosti korporativnykh sistem. // Otkrytye sistemy, №07-08, 2002.
7. Kalashnikov A.O., Kotukhov M.M., Lichmanov I.A. Prakticheskie voprosy audita sostoyaniya informatsionnoi bezopasnosti korporativnykh informatsionnykh sistem. // Information Security, №3, 2004.
8. Sheremet A.D., Suits V.P. Audit. – M.: Infra-M, 2005.
9. Gladkov Yu.M., Mikrin E.A., Shelkov A.B. Analiz i sintez mekhanizmov minimizatsii auditorskogo riska // Problemy upravleniya, №2, 2007.
10. Upravlenie riskami: obzor upotrebitel'nykh podkhodov. Chast' I. // «Jet Info», №11 (162), 2006.

DOI: 10.7256/2307-9118.2014.4.10281

11. Upravlenie riskami: obzor upotrebitel'nykh podkhodov. Chast' II // «Jet Info», №12 (163), 2006.
12. Saati T. Prinyatie reshenii. Metod analiza ierarkhii.-M.: Radio i svyaz'. 1993.
13. Macecrimmon K.P. Improving the system design and evaluation process by the use of trade of information: an application fourth last corridor transporta-tion planning RM 5877 – Dot // The Rand corporation. Cal.: Santa Monica. 1969.
14. Aizerman M.A., Malishevskii A.V. Problemy logicheskogo obosnovaniya v obshchei teorii vybora. Obshchaya teoriya vybora i ego klassichesko-ratsional'noe osnovanie. – M.: IPU RAN, 1980.
15. Podinovskii V.V., Nogin V D. Pareto-optimal'nye resheniya mnogokriterial'nykh zadach. – M.: Nauka, 1992.
16. Lopukhin M.M. PATTERN-metod planirovaniya i prognozirovaniya nauchnykh rabot. – M.: Sov. Radio, 1981.
17. Glotov V.A., Pavel'ev V.V. Vektornaya stratifikatsiya. – M.: Nauka, 1984.
18. Pavel'ev V.V. Formirovanie sistemy kriterial'nykh svoistv pri kompleksnoi otsenke slozhnykh ob''ektov / V kn.: Mekhanizmy funktsionirovaniya organizatsionnykh sistem. Vyp. 29. – M.: IPU RAN, 1982.
19. Levintal' A.B. i dr. Kompleksnoe otsenivanie i planirovanie razvitiya regiona. – M.: 2006.

DOI: 10.7256/2307-9118.2014.4.10281