УДК 004.056

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПОДДЕРЖКА ДЕЯТЕЛЬНОСТИ АУДИТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Надеждин Е.Н., [2]Новикова Т.Л.

[1]Государственный научно-исследовательский институт информационных технологий и телекоммуникаций, Москва, e-mail: e.nadezhdin@informika.ru;

[2]Шуйский филиал, Ивановский государственный университет, Шуя, e-mail: tshershakova@mail.ru

Статья посвящена проблеме автоматизации деятельности аудитора информационной безопасности. Изучены особенности реализации задач внутреннего аудита информационной безопасности в условиях конкретной образовательной организации. На основе содержательного описания построена формальная модель типового функционала аудитора информационной безопасности. В результате системного анализа и декомпозиции функциональной модели деятельности выделено подмножество информационно-аналитических задач, отличающихся повышенной сложностью и нелинейностью алгоритмов обработки и принятия решения. Выделены основные источники информации, которые традиционно используются аудитором для сбора исходных данных, анализа состояния защищённости сетевых ресурсов образовательной организации и подготовки отчёта. Показано, что одним из перспективных направлений повышения качества аудита является автоматизация решения информационно-аналитических задач. Для поддержки этого процесса предложено разработать набор специализированных интеллектуальных инструментов, который составит ядро программного обеспечения автоматизированного рабочего места аудитора информационной безопасности.

Ключевые слова: образовательная организация, аудит информационной безопасности, деятельность аудитора, функционал аудитора, интеллектуальные инструментальные средства

INFORMATION-ANALYTICAL SUPPORT OF ACTIVITY OF AUDITOR OF INFORMATION SECURITY

[1]Nadezhdin E.N., [2]Novikova T.L.

[1]State Institute of Information Technologies and Telecommunications, Moscow, e-mail: e.nadezhdin@informika.ru;

[2]Shuya branch of Ivanovo State University, Shuya, e-mail: tshershakova@mail.ru

The article is devoted the problem of automation of activity of public accountant of informative safety. The features of realization of tasks of internal audit of informative safety are studied in the conditions of concrete educational organization. On the basis of rich in content description the formal model of model functional of public accountant of informative safety is built. As a result of analysis of the systems and decouplig of functional model of activity a subset is selected informacionno-analiticheskie tasks, different enhanceable complication and nonlinearity of algorithms of treatment and decision-making. Basic information generators, which are traditionally used a public accountant for the capture of basic data, analysis of the state of protected of network resources of educational organization and preparation of report, are selected. It is rotined that one of perspective directions of upgrading audit is automation of decision of informacionno-analiticheskikh tasks. For support of this process it is suggested to develop the set of the specialized intellectual tools, which will make the kernel of workstation of public accountant of informative safety software.

Keywords: educational organization, information security audit, activity auditor, the auditor's functions, intelligent tools

Характерной чертой современного этапа информатизации системы высшего образования является активное развитие сетевой инфраструктуры образовательных организаций (ОО). В условиях непрерывного расширения спектра угроз и совершенствования технологий осуществления кибернетических атак на передний план выходят вопросы построения многоуровневой защиты сетевых ресурсов. Реалии информационного общества настоятельно требуют создания в каждой ОО интегрированной системы защиты информации (СЗИ) [4, 6].

Важным составным компонентом системы управления рисками информационной безопасности (ИБ), направленной на своевременное выявление, идентификацию и устранение уязвимостей в сетевой инфраструктуре ОО, является аудит информационной безопасности (АИБ) [1, 3]. В политике ИБ каждой ОО особое место отводится задачам АИБ, среди которых особое место занимают анализ функционального состояния аппаратно-программных средств информационно-вычислительной сети (ИВС) ОО и оценка защищённости её активов. Несмотря на возросший поток публикаций, посвящённых разработке технологий аудита, аккумулирующих положительный опыт оценки защищённости ИВС, по-прежнему

открытыми остаются вопросы рациональной организации, повышения качества и сокращения сроков проведения внутреннего АИБ ОО. Как показала практика, в условиях ограниченности привлекаемых ресурсов указанные показатели внутреннего АИБ существенно зависят от сложности объекта автоматизации, квалификации экспертов-аудиторов и характеристик используемых ими инструментальных средств.

Целью статьи является анализ перспективных направлений автоматизации информационно-аналитической деятельности аудитора и определение функций интеллектуальных инструментальных средств, способных в перспективе составить ядро программного обеспечения автоматизированного рабочего места (АРМ) аудитора ИБ.

Следуя рекомендациям нормативных документов, под аудитом информационной безопасности будем понимать системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ образовательной организации в соответствии с установленными требованиями и показателями безопасности [1].

Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Основными задачами АИБ являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИВС;
- оценка текущего уровня защищенности компонентов ИВС;
- локализация слабых звеньев в системе защиты информации;
- оценка соответствия СЗИ существующим стандартам в области ИБ;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов обеспечения ИБ;
- разработка (или корректировка) политики безопасности и других организационно-распорядительных документов по защите информации и их внедрению в деятельность ОО;
- конкретизация задач для ИТ-персонала в области защиты информации;
- разбор инцидентов, связанных с нарушением политики ИБ.

Выводы и рекомендации аудитора должны быть конкретными с учётом специфики ОО, экономически обоснованными, аргументированными и упорядоченными по степени важности. Как свидетельствует статистика, в ОО организационные мероприятия по обеспечению защиты информации практически всегда имеют приоритет над конкретными программно-техническими методами защиты. Поэтому принципиально важным следует считать выбор рабочей методики сбора и предварительный анализ информации о состоянии ИБ.

Выделим источники информации, используемые для проведения АИБ ОО [7]:

1) схема организационной структуры управления;
2) схема организационной структуры обслуживающих подразделений;
3) организационно-распорядительные документы по эксплуатации ИВС;
4) статистика инцидентов ИБ;
5) профили и учётные данные пользователей;
6) результаты моделирования конфликтных ситуаций;
7) материалы тестирования программного обеспечения;
8) результаты мониторинга ресурсов ИВС.

Определённую трудность при анализе состояния ИБ вызывает разнородность привлекаемых источников информации. Этап сбора данных в АИБ является наиболее сложным и трудоёмким. Это связано, прежде всего, с низким уровнем автоматизации процедур сбора и экстрагирования полезной информации и с необходимостью тесного взаимодействия аудитора со многими должностными лицами организации. Используемые аудиторами методы сбора и анализа данных определяются приоритетными задачами и выбранными подходами к проведению аудита, которые на практике могут существенно различаться.

Первый подход – *нормативный* – опирается на использование существующих стандартов ИБ и на практике сводится к определению группы индикаторов ИБ и к проверке их соответствия установленным требованиям. Второй подход – *аналитический* – базируется на определении, количественной оценке и анализе рисков ИБ. Опираясь на накопленный опыт оценки вероятных угроз и анализа рисков, аудитор определяет для обследуемой ОО индивидуальный набор требований ИБ, в наибольшей степени учитывающий особенности ИВС, среды её функционирования и существующие в данной среде угрозы безопасности. Данный подход, в отличие от нормативного подхода, является ресурсозатратным и требует

высокой квалификации аудитора. На продолжительность и качество аудита в этом случае сильно влияют принятая методология анализа рисков и её применимость к данному типу ИВС.

Анализ рисков включает в себя мероприятия по обследованию безопасности ИВС, с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Формирование набора адекватных контрмер осуществляется при разработке механизма управления рисками. Риск определяется вероятностью причинения ущерба или величиной ущерба, наносимого ресурсам ИВС, в случае осуществления угрозы безопасности. Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину, дав им качественную или количественную оценку.

Решение задачи анализа рисков можно разделить на четыре последовательных этапа:

1) оценка состояния ресурсов ИВС;

2) определение важности тех или иных ресурсов для ОО;

3) идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз;

4) определение рисков, связанных с осуществлением угроз безопасности.

В общем случае величина совокупного риска ИБ R_c определяется как взвешенная сумма частных рисков:

$$R_c = \sum_{k=1}^{m} \beta_k \cdot R_k;$$

$$\sum_{i=1}^{m} \beta_k = 1.$$

Здесь R_k – частный риск, заключающийся в нарушении целостности k-го ресурса; β_k – весовой коэффициент, отражающий важность соответствующего ресурса; m – число критических ресурсов.

Частный риск определяют на основе учёта стоимости рассматриваемого k-го ресурса, вероятности P_k осуществления угрозы и коэффициента уязвимости H_k ресурса по следующей формуле:

$$R_k = \frac{C_k \cdot P_k}{H_k}.$$

Задача управления рисками, как известно, заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. При этом стоимость реализации контрмер должна быть меньше величины возможного ущерба.

Пусть для проведения АИБ выбран второй подход, базирующийся на анализе рисков. Тогда на основе полученных данных выполняются следующие группы задач:

- анализ состояния всех видов ресурсов ИВС;
- анализ содержания задач, выполняемых существующей СЗИ;
- построение (неформальной) модели ресурсов ИВС, определяющей взаимосвязи между информационными, программными, техническими и людскими ресурсами, их взаимное расположение и способы взаимодействия;
- оценка критичности информационных, программных и технических ресурсов;
- определение критичности ресурсов с учетом их взаимозависимостей;
- идентификация наиболее вероятных угроз безопасности в отношении ресурсов ИВС и уязвимостей защиты, делающих возможным осуществление этих угроз;
- оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз;
- определение величины рисков для кортежа (угроза; группа ресурсов; уязвимость).

Комплекс задач, осуществляемых в процессе внутреннего АИБ, в зависимости от содержания рабочих процедур можно условно подразделить на следующие группы:

а) нормативно-проверочные;

б) информационно-статистические;

в) информационно-аналитические;

г) отчётно-оформительские.

Анализ практики проведения внутреннего АИБ ОО по схеме аналитического подхода показывает, что удельный вес указанных задач составляет соответственно 15…20, 36…45, 26…32 и 5…10%. В наибольшей степени сегодня автоматизированы задачи второй и четвёртой групп. Нормативно-проверочные операции предполагают непосредственную работу аудитора с конфиденциальными документами и при существующем уровне защищённости системы электронного документооборота их полная формализация нецелесообразна. Значительный ресурс в повышении оперативности и качества внутреннего АИБ заключается в автоматизации процесса решения информационно-аналитических задач [10], которые в конечном счёте и определяют обоснованность выводов и предложений по результатам аудита.

Информационно-аналитические задачи (ИАЗ) АИБ в силу их специфики следует отнести к классу некорректно поставленных задач принятия решений [9]. Их формализация обычно затрудняется следующими факторами: недостаток априорной информации, нечёткость задания критериев и ограничений, отсутствие стандартных вычислительных схем и базовых моделей, многомерность, многовариантность и индетерминизм. К группе ИАЗ следует отнести [2, 4]: комплексный анализ характеристик и формирование древовидной модели актуальных угроз безопасности на основе наблюдений, моделирования и экспертных оценок; выявление и ранжирование потенциальных уязвимостей в программном и аппаратном обеспечении; многокритериальная оценка эффективности механизмов защиты и выбор схем их адаптации; прогностическая оценка частных рисков ИБ (для различных активов); идентификация многофакторных моделей совокупного риска на основе нечёткого когнитивного моделирования; оптимизация комплекса организационных, программных, аппаратных, физических и иных мер защиты; идентификация семантической модели проблемной области ИБ сетевых ресурсов; генерация проектов предписаний и алгоритма действий администратора сетевой безопасности по устранению выявленных несоответствий нормативным требованиям. Несмотря на существенные отличия в постановке и способах решения, ИАЗ являются информационно-зависимыми задачами одной проблемной области. В интересах системной реализации ИАЗ обоснованным следует считать создание пакета прикладных программ, включающего набор семантических моделей и процедур поддержки задач анализа рисков и имеющего единую информационную базу. По мнению ряда экспертов, задачи моделирования и анализа информационных рисков в процессе АИБ относятся к классу наиболее трудоёмких аналитических задач и требуют высокой квалификации аудитора [1, с. 23]. При этом наибольшие трудности заключаются в построении адекватных моделей частных информационных рисков и совокупного риска для активов ОО, что обусловлено неполнотой, недостоверностью и противоречивостью используемой информации. В качестве платформы для разработки интеллектуального инструментария количественной оценки рисков ИБ могут быть рекомендованы апробированные на практике технологии нейросетевого моделирования и нечёткого когнитивного анализа [2, 5, 9]. В ходе нашего исследования было установлено, что одним из перспективных способов повышения точности прогностических оценок рисков ИБ может служить введение в состав программного обеспечения АРМ специальных процедур для комплексной обработки и цифровой фильтрации исходной информации, поступающей от различных источников.

В целях конкретизации функционала инструментальных программных средств АРМ аудитора выполним следующие действия. Предположим, что на первом этапе аудита процедуры сбора, предварительной обработки, накопления и агрегирования исходных данных и идентификации состояния ИБ выполнены в полном объёме. Тогда на последующих этапах аудита функции аудитора сводятся к решению определённого набора задач статистического анализа и оптимизации с применением стандартных вычислительных методов, к подготовке на их основе выводов и рекомендаций и к документированию результатов.

Пусть модель программного обеспечения АРМ представлена кортежем:

$$R = (L, P, M, F),$$

где L – интерфейс, поддерживающий взаимодействие пользователя с программным обеспечением АРМ; P – прикладные программы-модули, обеспечивающие численное решение задач из некоторой предметной области; M – информационная модель предметной области, определяемая совокупностью прикладных проблем, сводимых к некоторому множеству частных задач, которые обладают общностью применяемых алгоритмов решения и информационных массивов; F – управляющая программа, выполняющая роль специализированной операционной системы.

Предметную область априорно будем считать заданной в виде

$$M = (D, Z, A, Q),$$

где $D = \{D_k,\ k = \overline{1,K}\}$ – множество типовых структур наборов исходных данных; $Z = \{Z_j,\ j = \overline{1,J}\}$ – класс задач, образованный множеством типовых задач обработки и анализа данных; $A = \{A_i,\ i = \overline{1,I}\}$ – множество алгоритмов, при этом A_i являются до конца формализованными, допускающими

численную реализацию на ЭВМ и представление в виде конечной последовательности программных модулей [8, с. 19]; *Q* – множество ограничений и требований, соблюдение которых связано с содержанием решаемых частных задач и считается необходимым.

В указанной постановке основные задачи АИБ могут быть полностью автоматизированы. Для эффективной реализации в АРМ аудитора отмеченных особенностей предметной области потребуется найти решение нескольких нетривиальных аналитических задач:

а) идентификация массивов данных по материалам пассивного и активного мониторинга сетевых ресурсов и функционального состояния компонентов ИВС;

б) комплексная обработка и оценивание разнородных данных;

в) кластеризация информационных угроз и оценка их характеристик;

г) идентификация моделей и анализ частных рисков ИБ;

д) выявление скрытых уязвимостей в компонентах сетевой инфраструктуры ОО.

Указанные выше задачи в силу своей природы и отсутствия стандартных методов решения следует отнести к группе интеллектуальных задач [9].

Внутренний АИБ проводится, как правило, силами и средствами самой ОО. Ограниченность привлекаемых для осуществления задач внутреннего АИБ материальных и административных ресурсов и лимит времени, выделяемого на проверку оборудования и анализ документации и статистики инцидентов без нарушения штатного процесса функционирования ИВС, существенно ограничивают объёмы выполняемых исследований. В результате действия указанных факторов мероприятия внутреннего АИБ проводятся в ускоренном режиме и нередко носят фрагментарный характер. Негативное влияние на глубину анализа, объективность результатов аудита и обоснованность выводов и рекомендаций оказывают профессиональная неподготовленность привлекаемых штатных сотрудников ОО и отсутствие у них достаточного опыта и навыков в планировании и проведении подобных аналитических исследований.

Из практики аудита безопасности информационных систем вытекают основные критерии качества аудиторского заключения [1]: достоверность, актуальность, ясность и полезность, которые по своей природе противоречивы и предполагают поиск компромиссного решения. Компьютерная реализация набора ИАЗ на основе применения специальных инструментальных средств, поддерживающих дополнительные интеллектуальные функции (нечёткий когнитивный анализ, параметрическая идентификация, экспертные оценки, обучение и самообучение, ранговая классификация и др.), поможет существенно повысить продуктивность работы эксперта-аудитора и, как следствие, обеспечить высокое качество АИБ.

Таким образом, в результате анализа и декомпозиции функционала аудитора информационной безопасности выделены три группы функциональных задач, которые наиболее перспективны с точки зрения их автоматизации в составе АРМ:

1) организационные;

2) информационно-статистические;

3) информационно-аналитические (интеллектуальные).

Организационные задачи регламентируются известными нормативными документами с учётом существующей организационно-штатной структуры ОО и её сетевой инфраструктуры. Информационно-статистические задачи могут быть сведены к накоплению, обработке и статистическому анализу на основе известных методов и алгоритмов теории вероятностей и математической статистики. Интеллектуальные задачи предполагают применение эвристических подходов с использованием специальных процедур поддержки принятия решений. Для их компьютерной реализации могут быть привлечены семантические сети и нечёткие когнитивные модели, интегрирующие опыт экспертов в постановке и решении подобных задач и допускающие выбор предпочтительного варианта в соответствии с функцией предпочтения аудитора.

Список литературы

1. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов. – 2-е изд., стереотип. – М.: ФЛИНТА, 2011. – 269 с.

2. Ахметов Ю.М. Принципы разработки эффективного инструмента аудита безопасности информационных систем // Информационное противодействие угрозам терроризма. Научно-практический журнал. – 2010. – no. 14. – С. 21–26.

3. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. – М.: БДЦ-Пресс, 2006. – 304 с.

4. Надеждин Е.Н. Проблемные вопросы интеллектуализации информационных систем образовательного назначения // Информационные ресурсы в образовании: материалы Международной научно-практической конференции (г. Нижневартовск, 17–19 апреля 2013 г.). – Нижневартовск: НВГУ, 2013. – С. 8–11.

5. Надеждин Е.Н., Шептуховский В.А. Методика оценивания рисков информа-ционной безопасности в вычислительных сетях образовательных учреждений // Педаго-гическая информатика. – 2012. – no. 4. – С. 84–92.

6. Надеждин Е.Н., Смирнова Е.Е., Шершакова Т.Л. Математические основы моделирования и анализа интегрированных систем защиты информации: учебное пособие. – Тула: НОУ ВПО «Московский институт комплексной безопасности». Изд-во ТулГУ. – 205 с.

7. Новикова Т.Л., Надеждин Е.Н. Информационное обеспечение внутреннего аудита информационной безопасности образовательной организации // Комплексная защита объектов информатизации: сб. науч. трудов Всероссийской научно-практической конференции с межд. участием 1-5.06.2016 года. – СПб.: Изд-во политехн. ун-та, 2016. – С. 48–51.

8. Парасюк И.Н., Сергиенко И.В. Пакеты программ анализа данных: технология разработки. – М.: Финансы и статистика, 1988. – 159 с.

9. Романов В.П. Интеллектуальные информационные системы в экономике: учебное пособие / под ред. Н.П. Тихомирова. – М.: Изд-во «Экзамен». – 2003. – 496 с.

10. Шершакова Т.Л. Задачи внутреннего аудита информационной безопасности университета в контексте реализации системы менеджмента качества образовательных услуг // Научный поиск. – 2013. – no. 2.5. – С. 31–33.

References

1. Averchenkov V.I. Audit informacionnoj bezopasnosti: ucheb. posobie dlja vuzov. 2-e izd., stereotip. M.: FLINTA, 2011. 269 p.

2. Ahmetov Ju.M. Principy razrabotki jeffektivnogo instrumenta audita bezopasno-sti informacionnyh sistem // Informacionnoe protivodejstvie ugrozam terroriz-ma. Nauchno-prakticheskij zhurnal. 2010. no. 14. pp. 21–26.

3. Kurilo A.P., Zefirov S.L., Golovanov V.B. Audit informacionnoj bezopasnosti. M.: BDC-Press, 2006. 304 p.

4. Nadezhdin E.N. Problemnye voprosy intellektualizacii informacionnyh sistem obrazovatelnogo naznachenija // Informacionnye resursy v obrazovanii: materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii (g. Nizhnevartovsk, 17–19 aprelja 2013 g.). Nizhnevartovsk: NVGU, 2013. pp. 8–11.

5. Nadezhdin E.N., Sheptuhovskij V.A. Metodika ocenivanija riskov informa-cionnoj bezopasnosti v vychislitelnyh setjah obrazovatelnyh uchrezhdenij // Pedago-gicheskaja informatika. 2012. no. 4. pp. 84–92.

6. Nadezhdin E.N., Smirnova E.E., Shershakova T.L. Matematicheskie osnovy modeliro-vanija i analiza integrirovannyh sistem zashhity informacii: uchebnoe posobie. Tula: NOU VPO «Moskovskij institut kompleksnoj bezopasnosti». Izd-vo TulGU. 205 p.

7. Novikova T.L., Nadezhdin E.N. Informacionnoe obespechenie vnutrennego audita informacionnoj bezopasnosti obrazovatelnoj organizacii // Kompleksnaja zashhita obektov informatizacii: sb. nauch. trudov Vserossijskoj nauchno-prakticheskoj konferencii s mezhd. uchastiem 1-5.06.2016 goda. SPb.: Izd-vo politehn. un-ta, 2016. pp. 48–51.

8. Parasjuk I.N., Sergienko I.V. Pakety programm analiza dannyh: tehnologija razra-botki. M.: Finansy i statistika, 1988. 159 p.

9. Romanov V.P. Intellektualnye informacionnye sistemy v jekonomike: uchebnoe po-sobie / pod red. N.P. Tihomirova. M.: Izd-vo «Jekzamen». 2003. 496 p.

10. Shershakova T.L. Zadachi vnutrennego audita informacionnoj bezopasnosti univer-siteta v kontekste realizacii sistemy menedzhmenta kachestva obrazovatelnyh uslug // Nauchnyj poisk. 2013. no. 2.5. pp. 31–33.