УДК 334.02:65.011.56

Проектирование эффективной системы информационной безопасности предприятия

Канд. экон. наук **Волкодаева А.В.** arina-21@mail.ru
НОУ ВПО Самарский институт управления
443013, г Самара, ул. Дачная, 28.

В статье рассматривается порядок проектирования эффективной системы информационной безопасности с использованием концептуальной схемы, где одним из важных этапов является проведении диагностического обследования системы информационной безопасности. Проектирование системы информационной безопасности тесно связано ее архитектурой, в частности с соблюдением баланса между инвестициями уровнем ее защиты. В статье рассмотрены регламентированные этапы по проектированию системы информационной безопасности предприятия, а также рассмотрены механизмы внедрения, сопровождения и обслуживания системы. Рассматриваются положительные и отрицательные стороны привлечения внешних специалистов и создания собственных структур по управлению информационной безопасность предприятия. Организационным аспектом обеспечения информационной безопасности предприятия определяется необходимость анализа и мониторинга состояния информационной безопасности с дальнейшим принятием своевременных и объективных защитных мер.

Ключевые слова: система информационной безопасности предприятия, защита информации, диагностика, проектирование, аутсорсинг.

Design of effective system information security of the enterprise

Ph.D. **Volkodayeva A.V.** arina-21@mail.ru
Samara institute of management
443013, Samara, Dachnaya St., 28.

In article the order of design of an effective information security system with use of the conceptual scheme where one of important stages is carrying out diagnostic inspection of an information security system is considered. Design of an information security system is closely connected by its architecture, in particular with observance of balance between investments the level of its protection. In article the regulated stages on design of an information security system of the enterprise are considered, and also mechanisms of introduction, maintenance and service of system are considered. Positive and negative sides of involvement of external experts and creation of own structures on management information safety of the enterprise are considered. Need of the analysis and monitoring of a condition of information security decides on further acceptance of timely and objective protective measures by organizational aspect of ensuring information security of the enterprise.

Keywords: information security system of the enterprise, information security, diagnostics, design, outsourcing.

Единой оптимальной структуры защиты информации не существует, так как каждая организация-участник информационных процессов имеет свой собственный отличающийся от других набор требований, проблем и приоритетов, продиктованных объективными экономическими, производственными, социальными условиями функционирования данного предприятия. Поэтому основополагающим моментом создания на предприятии системы обеспечения информационной

безопасности является разработка и реализация уникальной, максимально адаптированной к конкретным условиям политики информационной безопасности [1].

Осуществляя проектирование эффективной системы информационной безопасности или ее модернизацию, следует руководствоваться существующей концептуальной схемой эффективной системы информационной безопасности, представленной на рисунке 1.Согласно обозначенным этапам схемы, выполняются конкретные действия, которые в совокупности представляют собой целостное системное взаимодействие технических, технологических, организационных, экономических и правовых мероприятий, обеспечивающих необходимый уровень информационной безопасности.

1) Диагностическое обследование/аудит системы информационной безопасности.

Для построения эффективной системы информационной безопасности, выбор и внедрение адекватных технических средств защиты должен предваряться анализом угроз, уязвимостей информационной системы и на их основе - анализом рисков информационной безопасности. Выбор программно-аппаратного обеспечения защиты и проектирование систем информационной безопасности основывается на результатах такого анализа с учетом экономической оценки соотношения «стоимость контрмер по снижению рисков/возможные потери промышленного предприятия от инцидентов информационной безопасности».

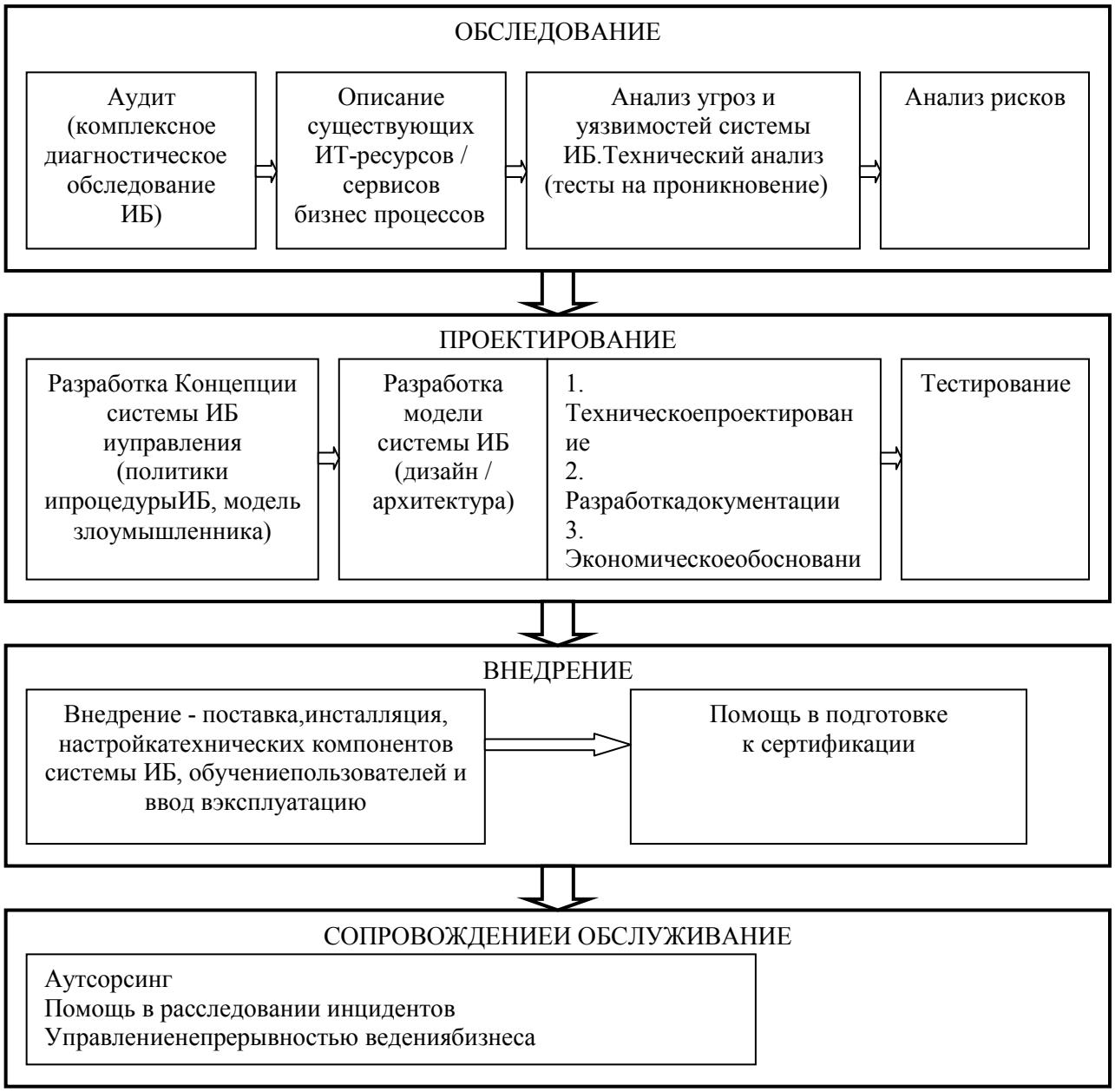
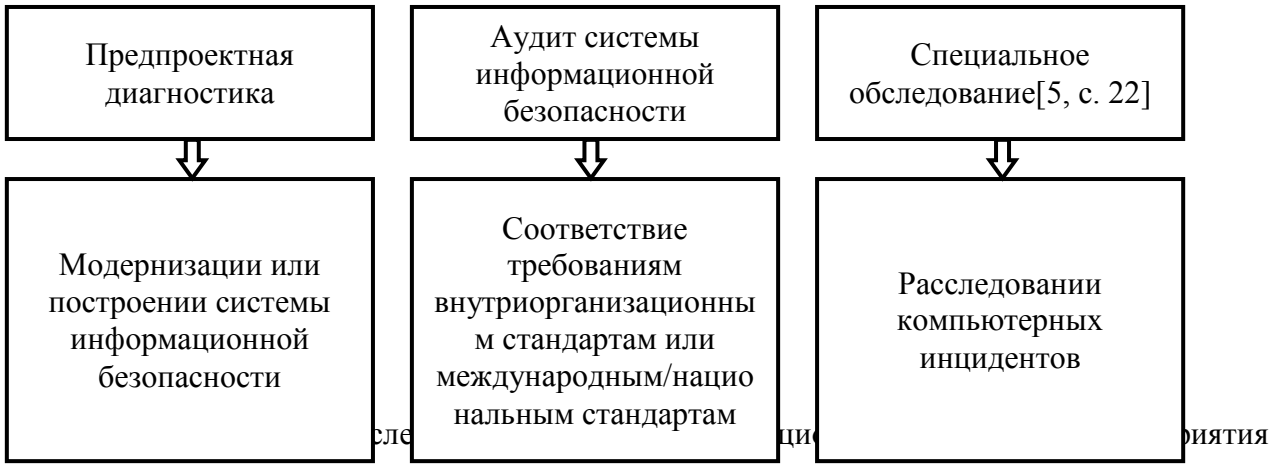


Рис.1. Концептуальная схема построения эффективной системы информационной безопасности [2, с. 192]

Концептуальная схема построения эффективной системы информационной безопасности определяет, что построение последней важно начинать проведения комплексной диагностики основных бизнес-процессов предприятия и его информационной системы в целом[3].Диагностика системы информационной безопасности предприятия даст возможность определить уровень безопасности информационно-технологических ресурсов промышленного предприятия и соотнести их с предъявляемыми требованиями согласно параметрам конфиденциальности, доступности и целостности ресурсов информационной системы. Также, проведение комплексной диагностики позволит выявить возможные и риски и определить мероприятия по противостоянию несанкционированному доступу и воздействию на информацию предприятия[4, с. 129].Диагностика может осуществляться согласно нескольким видам обследования (рисунок 2).



При проведении диагностического обследования/аудита системы информационной безопасности последовательно выполняются следующие работы (рисунок 3).

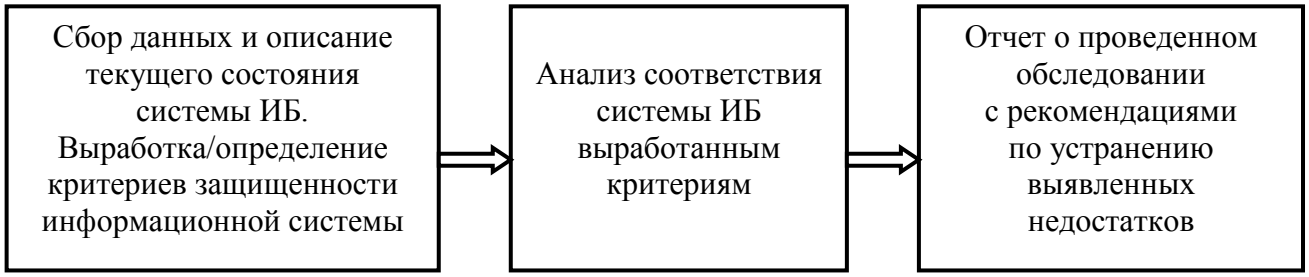


Рис. 3. Последовательность работ при проведении аудита системы информационной безопасности [6]

Каждый этап работ имеет реальные, контролируемые результаты, что позволяет обеспечить эффективный контроль проекта на всем его протяжении.

В процессе обследования и анализа системы информационной безопасности также идентифицируются «владельцы» информационных активов (включая автоматизированные системы и данные предприятия) и лица, ответственные за целостность этих ресурсов. Устанавливаются требования к системе разделения прав доступа (пароли, разрешения), включая все правила доступа к информационной системе промышленного предприятия. Информационные активы классифицируются по степени важности/критичности.

Проверяются все процедуры безопасности, в том числе поддержка системы информационной безопасности, процесс расследования нарушений информационной безопасности, организация системы резервного копирования, разграничение прав пользователей, процедуры удаленного доступа, защиты учетных записей и др. Определяются лица, ответственные за развитие и поддержку системы

информационной безопасности.

В ходе анализа и моделирования возможных сценариев атак на систему информационной безопасности выявляются ситуации, которые могут привести к нарушению нормального «течения» бизнес-процессов. Определяются возможные последствия несоответствия системы информационной безопасности политике безопасности предприятия. Если обследование выполняется сторонней организацией, то на всех стадиях проекта необходимо привлечение к работам персонала компании-заказчика. Это гарантирует учет основных требований, специфики и интересов обследуемого предприятия.

Существенным преимуществом привлечения к аудиту внешнего исполнителя (компании-интегратора) является возможность использования накопленного консультантом опыта при анализе каждого компонента системы информационной безопасности на соответствие требованиям но обеспечению информационной безопасности, в том числе и с позиции «лучшей практики» для конкретной индустрии. Однако в таком случае о системе защиты, применяемых мерах и средствах, слабых и сильных сторонах становится известно третьей стороне. Это уже является существенным недостатком.

По завершении обследования руководителям и заинтересованным менеджерам представляется детальный отчет с рекомендациями по изменению или дополнению существующей инфраструктуры системы информационной безопасности. Составляется список необходимых мероприятий по обеспечению информационной безопасности в соответствии с требованиями международных (ISO 17799, ISO 13335) или национальных стандартов (Стандарт ЦБ РФ, СТР-К, NIST SP800-14, BSI и др.), техническими требованиями поставщиков решений в области информационной безопасности (CISCO, CheckPoint и др.), рекомендациями NSA (NationalSecurityAgency).

2) Проектирование системы информационной безопасности.

На данном этапе этапом построения системы информационной безопасности осуществляется ее проектирование, в том числе и проектирование системы управления информационной безопасности[7].

Задача проектирования системы информационной безопасности тесно взаимосвязана с понятием архитектуры системы информационной безопасности. Архитектурасистемы информационной безопасности является интегрированным решением, соблюдения баланса между инвестициями в систему информационной безопасности и обеспечением соответствующего уровня ее защиты. Среди ее преимуществ, можно обозначить интеграцию подсистем, позволяющую снизить совокупную стоимость владения системой, повысить окупаемость инвестиций при внедрении и улучшение управляемости системы информационной безопасности[8, с. 26].

Высокая эффективность системы информационной безопасности может быть достигнута, если все ее компоненты представлены качественными решениями, функционируют как единый комплекс и имеют централизованное управление. Система безопасности должна строиться на основе анализа рисков, и стоимость ее внедрения и поддержки должна быть адекватной существующим угрозам, то есть экономически обоснованной.

Архитектура системы информационной безопасности предприятия включает в себя систему управления информационной безопасностью, в частности сами процессы и процедуры по ее обеспечению.Так, в задачи системы управления информационной безопасностью включено:

- структурирование и систематизация процессов обеспечения информационной безопасности;
- определениеосновных приоритетных направленийпредприятия по обеспечению информационной безопасности;
- достижение «прозрачности» и адекватности системы информационной безопасности предприятия;

Обозначенные задачи имеют высокую степень важности, поскольку их реализация позволяет четко определитьвзаимосвязи процессов и подсистем информационной безопасности предприятия, в том числе ответственных лиц, потоки финансовых и человеческих ресурсов для ее обеспечения, что

позволяет отслеживать изменения в системе, выполнение политики безопасностии в конечном счете эффективно управлять системой в критичных ситуациях [2, с. 196].

В целом, процесс управления безопасностью (SecurityManagement) отвечает за планирование, исполнение, контроль и техническое обслуживание всей инфраструктуры безопасности. Организация этого процесса усложняется тем обстоятельством, что обеспечение информационной безопасности промышленного предприятия связано не только с защитой информационных систем и бизнес-процессами, которые поддерживаются этими информационными системами. У предприятия часто существуют бизнес-процессы, не связанные с информационными технологиями, но попадающие в сферу обеспечения информационной безопасности, например, процессы кадровой службы по найму персонала.

Существует ряд регламентированных этапов по проектированию системы информационной безопасности предприятия:

Первый этап включает разработку политики обеспечения информационной безопасности предприятия. Здесь ставятся основные цели, определяются задачи и требования к системе информационной безопасности, а также в целом определяется общая стратегия построения системы информационной безопасности. В рамках общей стратегии важными моментами являются определение критичных информационных ресурсов для системы и требований к ее обеспечению, что определяет соответствующие базовые подходы к их реализации.

На втором этапе непосредственно создается (развивается) политика информационной безопасности предприятия.

Далее, уже на третьем этапе проектирования, строится модель системы управления информационной безопасности.

Четвертый этап включает уже подготовку технического задания непосредственно на создание системы информационной безопасности.

На пятом этапе данная модель создается.

Важным является шестой этап проектирования системы информационной безопасности предприятия, так как здесь разрабатывается технический рабочий проект создания системы информационной безопасности и архитектуры системы информационной безопасности. Технический рабочий проект включает:

- пояснительную записку (характеристика технических решений по созданию системы информационной безопасности и организационно-управленческих мероприятий по ее подготовке к эксплуатации);
- обоснование выбранных компонентов системы информационной безопасности и определение мест их размещения;
- характеристику разработанных профилей информационной защиты
- спецификацию на техническиеи программные средства системы информационной безопасности;
- определение настроек и режима функционирования компонентов системы информационной безопасности.

На седьмом этапе осуществляется тестирование проектной системы информационной безопасности.

Далее (на восьмом этапе) разрабатываются организационно-распорядительных документов системы управления информационной безопасности, включающие процедуры, регламенты и др.

Заключительный (девятый) этап включает разработку рабочего проекта и планирование обучения персонала, использующегоинформационную систему [9, с. 94-96].

3) Внедрение системы информационной безопасности.

После проведения полного тестирования спроектированной системы информационной безопасности, можно приступать к ее внедрению. Работы по внедрению системы включают выполнение

следующих задач: поставку программных и технических средств защиты информации; инсталляцию программных компонентов; настройку всех компонентов и подсистем; проведение приемо-сдаточных испытаний; внедрение системы управления информационной безопасности; обучение пользователей; ввод системы информационной безопасности в промышленную эксплуатацию.

Для эффективной дальнейшей эксплуатации системы необходимо обеспечить ее поддержку и сопровождение (собственными силами предприятия или силами привлекаемых специалистов).

4) Сопровождение и обслуживание.

При осуществлении мероприятий по созданию или модернизации системы информационной безопасности предприятия порой возникает необходимость привлечения внешних консультантов. Однако, отдавать на аутсорсинг процессы обеспечения информационной безопасности необходимо только при условии, если она не является основной бизнеса.

В то же время серьезным аргументом в пользу привлечения аутсорсера служит его объективность. Можно быть более или менее уверенным, что он будет непредвзято отслеживать нарушителей и сообщать обо всех действиях, невзирая на их статус внутри предприятия.

Важно выбрать надежного партнера, который будет отвечать следующим требованиям:

- хорошая репутацию на рынке;
- серьезный опыт работы в сфере информационной безопасности самой компании и отдельных ее сотрудников;
- наличие в компании программных и технических средств для проектирования и моделирования системы информационной безопасности, в том числе и наличие партнерских отношений с поставщиками необходимых программных и технических средств;
- наличие круглосуточного центра технической поддержки, включающего услуги аутсорсинга, удаленный мониторинг средств защиты информации и др.

Обеспечение безопасности информации требует постоянного присутствия специалиста на предприятии, его доступа к весьма чувствительным с точки зрения безопасности объектам, общения с сотрудниками и пользователями информационной системы. Получается, что специалист вроде бы «наш», а вроде бы и «не наш». Да и с экономической точки зрения такой аутсорсинг эквивалентен приему на работу собственного специалиста. Так кого лучше содержать: своего или чужого? А если надо срочно принять серьезное управленческое решение по восстановлению нарушенной безопасности информации?

Процесс обеспечения информационной безопасности предприятия является непрерывным. В него включено управление средствами защиты, ресурсами предприятия, рисками, и т.д. Человеческий ресурс является неотъемлемой частью автоматизированной системы управления информационной безопасностью предприятия и обеспечивает эффективность ее функционирования[10].

Организационный аспект обеспечения информационной безопасности промышленного предприятия является одним из важнейших элементов информационной безопасности, так как от его реализации в значительной степени зависит эффективность всей деятельности по поддержанию системы информационной безопасности на должном уровне. То есть правильное решение вопросов создания органов информационной безопасности будет способствовать ускорению комплексного внедрения и поддержанию работоспособности целостной системы информационной безопасности, увязывающей правовые, административные, организационные, технологические, научно-технические и физические меры защиты информации. Организационный аспект существенным образом влияет на проведение внутреннего аудита информационной безопасности, ведение объективного анализа и мониторинга состояния информационной безопасности с выявлением нарушений и новых угроз информационной безопасности, на своевременное и объективное расследование этих нарушений с принятием защитных мер и определением степени вины сотрудников и других лиц. Роль организационного аспекта тем более возрастает, чем выше уровень зрелости промышленного

предприятия по обеспечению процессов информационной безопасности, чем выше степень осознания основной специфики вопросов информационной безопасности, заключающейся в том, что проблема информационной безопасности является междисциплинарной темой, охватывающей фактически все аспекты бизнеса предприятия.

Список литературы

1. *Трифаленков И.А.* Текущее состояние проблемы информационной безопасности // Итоги конференции: «Актуальные проблемы информационной безопасности: подходы и решения». 2003. URL: http://citforum.ru/seminars/security2003/index.shtml (дата обращения 26.02.2011 г.)

2. *Балановская А.В., Волкодаева А.В.* Организационно-экономические механизмы обеспечения эффективности управления информационной безопасностью промышленных предприятий: монография. Самара: САГМУ, 2012. 248 с.

3. *Жук Е.И.* Концептуальные основы информационной безопасности // Электронное научно-техническое издание «Наука и образование». 2010. № 4. URL: http://technomag.stack.net/doc/143237.html (дата обращения: 17.01.2014 г.)

4. *Казакова А.В.* Концепция информационной безопасности промышленных предприятий // Вестн. Самар. гос. ун-та. - Самара, 2011. № 3 (84). С. 128-135.

5. *Кондрахин О.Ю.,* Тестовые режимы для проведения специальных исследований // Технические средства защиты информации: Тезисы докладов VIII Белорусско-российской научно-технической конференции, 24-28 мая 2010 г., г. Браслав. Минск: БГУИР, 2010. 150 с.

6. *Казакова А.В.* Развитие системы обеспечения информационной безопасности промышленных предприятий: автореферат // Экономическая библиотека. URL: http://economy-lib.com/razvitie-sistemy-obespecheniya-informatsionnoy-bezopasnosti-promyshlennyh-predpriyatiy#1 (дата обращения: 09.12.2011 г.)

7. *Голов А.* Интегрированная архитектура системы информационной безопасности // Connect! Мир Связи. 2006. № 9. URL: http://www.connect.ru/article.asp?id=7120

8. *Глущенко Д.В., Урядов В.Н.,* Архитектура PON с точки зрения информационной безопасности // Технические средства защиты информации: Тезисы докладов VIII Белорусско-российской научно-технической конференции, 24-28 мая 2010 г., г. Браслав. Минск: БГУИР, 2010. 150 с.

9. *Казакова А.В.* Организационные механизмы разработки и управления информационной безопасностью промышленных предприятий: монография / А.В. Балановская, А.В. Казакова. - Самара : Изд-во Самар. ин-та управления, 2010. 138 с. - С. 94-96.

10. *Казакова А.В.* Развитие системы обеспечения информационной безопасности промышленных предприятий // Вестник самарского государственного экономического университета. 2011. № 5 (79). URL: http://vestnik.sseu.ru/view_pdf.php?pdf (дата обращения 03.03.2014 г.)

References

1. Trivalence I. A. the Current state of information security issues // the results of the conference "Actual problems of information security: approaches and solutions. 2003. URL: http://citforum.ru/seminars/security2003/index.shtml (accessed on 26.02.2011,)

2. Balanovskaya, A.V., Volkodaeva A.V. Organizational-economic mechanisms ensuring the effectiveness of information security management of industrial enterprises: monograph. Samara: SAGA, 2012. 248 C.

3. Zhuk E. I. Conceptual foundations of information security // Electronic scientific-technical journal "Science and education". 2010. No. 4. URL: http://technomag.stack.net/doc/143237.html (date of access: 17.01.2014 g)

4. Kazakova A. V. the Concept of information security of industrial enterprises // *VestnikSt.Petersburg University. Samar.state University.* - Samara, 2011. No. 3 (84). C. 128-135.

5. Kondrakhin O. Y., Test modes for carrying out special studies // Technical information protection: abstracts of the VIII Belarusian-Russian scientific-technical conference, may 24-28, 2010, ,Braslav. Minsk: BSUIR, 2010. 150 C.

6. Kazakova A. V. development of a system of information security of industrial enterprises: abstract // the Economic library. URL: http://economy-lib.com/razvitie-sistemy-obespecheniya-informatsionnoy-bezopasnosti-promyshlennyh-predpriyatiy#1 (date of access: 09.12.2011,)

7. Goals A. Integrated system architecture information security // Connect! Communication World.2006. No. 9. URL: http://www.connect.ru/article.asp?id=7120

8. Glushchenko D. C., Uryadov C. N., The PON architecture from the point of view of information security // Technical information protection: abstracts of the VIII Belarusian-Russian scientific-technical conference, may 24-28, 2010, , Braslav. Minsk: BSUIR, 2010. 150 C.

9. Kazakova A. V. Organizational development mechanisms and information security management of industrial enterprises: monograph / A. Balanov, A. B. Kazakova. - Samara : Publishing house of Samar. Institute of management, 2010. 138 C. - S. 94-96.

10. Kazakova A. C. Development of a system of information security of industrial enterprises // *Vestnik of Samara state economic University.* 2011. No. 5 (79).

Статья поступила в редакцию 06.04.2015 г.