

1 Применение программных средств управления безопасностью

Деятельность по обеспечению информационной безопасности на предприятии может поддерживаться программными продуктами различных типов. В большинстве случаев программная поддержка реализации политики информационной безопасности обеспечивается функциями и программными модулями, которые встроены непосредственно в программное обеспечение, создающее условия для хранения, обработки и передачи информации (операционные системы, системы управления базами данных, системы электронной почты, MRP/ERP-системы). Практически все современные программные продукты имеют внутренние средства, позволяющие четко определить права тех или иных пользователей, разграничить доступ к информации, распределить использование системных ресурсов и ввести другие ограничения, которые в целом должны обеспечить соблюдение установленных требований и реализацию политики информационной безопасности.

Применение других инструментальных средств, как правило, не является обязательным, но во многих случаях позволяет повысить эффективность и качество многих работ, связанных с оценкой рисков, разработкой организационной документации, контролем за выполнением установленных требований и выполнением многих других важных функций. Таким образом, выделяется отдельный класс специальных программных продуктов, предназначенных исключительно для поддержания процессов разработки политик безопасности и управления информационной безопасностью на организационном уровне. Основными функциями таких программ являются справочно-информационная поддержка, помощь при обработке управленческой информации, оценке рисков и подготовке необходимых документов. В частности, для этих целей может использоваться ПО следующих основных видов:

- сборники (интерактивные электронные справочники), которые содержат типовые документы (шаблоны документов), используемые для

Тема 2.8 – Программные средства планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)

управления информационной безопасностью, описания отдельных процессов и процедур, связанных с обеспечением информационной безопасности, должностных обязанностей и функций сотрудников предприятия;

- системы, предназначенные для накопления и обработки сведений о рисках и проведения сводных оценочных расчетов показателей риска;

- ПО, интегрированное в информационную систему предприятия и позволяющее автоматически контролировать соблюдение установленных политик безопасности, а также помогающее формировать заключения о текущем состоянии информационной безопасности (в т.ч. путем анализа действий пользователей в информационной системе, а также путем анализа журналов операционных систем, программ, средств защиты и сетевого оборудования);

- ПО, осуществляющее поддержку процессов аудита информационной безопасности.

Также с управлением информационной безопасностью связаны программные продукты, которые:

- автоматически (централизованно и унифицировано) управляют учетными записями и правами доступа одновременно в нескольких элементах информационной инфраструктуры (базах данных, приложениях и пр.);

- производят автоматическое сканирование отдельных элементов информационной инфраструктуры (операционных систем, программ, средств защиты информации) и их проверку на устойчивость и наличие уязвимостей;

- производят автоматическое обновление программных продуктов с целью устранения выявленных уязвимостей (установку т.н. «патчей», «заплаток»).

2 Программная поддержка политики безопасности

Сборники (справочники), которые содержат типовые документы, связанные с обеспечением информационной безопасности, могут включать в себя:

- образцы политик безопасности разных уровней для предприятий, функционирующих в различных сферах деятельности и предъявляющих различные требования к уровню защищенности информации;
- образцы (шаблоны, бланки) документов, используемых в процессах защиты информации (обязательств о неразглашении информации, отчетов о состоянии информационной безопасности и пр.);
- образцы разделов различных договоров (контрактов с различными контрагентами или трудовых договоров с сотрудниками предприятия), содержащие требования к обеспечению информационной безопасности.

Такого рода электронные справочники могут выпускаться как на основе оригинальных методических разработок, так и на основе общепризнанных стандартов (таких как ISO 17799) с целью содействовать прохождению сертификации на соответствие этим стандартам. Выпускаемые электронные справочники могут быть дополнены учебниками, текстами стандартов и другими методическими материалами, выпущенными в виде брошюр. Одним из наиболее полных является электронный справочник «Information Security Policies Made Easy» американской компании Information Shield, Inc. Девятая версия этого справочника содержит более 1360 образцов и шаблонов различных документов, созданных с учетом требований стандарта ISO 17799 и относящихся ко всем аспектам информационной безопасности предприятия.

Концепции более развитых программных продуктов, основанных на интерактивном интеллектуальном анализе и совершенствовании политики безопасности, предполагают, что пользователь (менеджер) сначала внесет всю необходимую информацию о состоянии информационной безопасности на своем предприятии (ответит на задаваемые программой вопросы), а затем

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

получит детальный отчет о состоянии информационной безопасности, описание уровня соответствия требованиям стандартов, рекомендации по усовершенствованию действующей политики безопасности и другие отчеты. Таким образом, программное обеспечение позволяет увязывать в единый процесс процедуры первичного сбора информации о предприятии, анализа фактического уровня организационного обеспечения информационной безопасности, разработки документации, адаптации методов управления к определенным требованиям (например, стандарта ISO 17799) и проведение аудитов информационной безопасности.

Одним из таких программных продуктов является система «COBRA», поставляемая британской компанией «C&A Systems Security Ltd.» в двух вариантах: сокращенная версия включает в себя модуль «COBRA ISO17799 Consultant», а полная версия, помимо него, содержит также дополнительные средства анализа рисков («Risk Consultant») и специальный модуль, позволяющий создавать и модифицировать собственные базы знаний и наборы вопросов для исследования состояния информационной безопасности («Module Manager»). Базовый модуль этой системы предназначен для оценки того, в какой степени работа по защите информационной безопасности соответствует требованиям стандарта ISO 17799. На первом этапе его использования вступает в работу «Question Module» – Модуль ответов на вопросы, который содержит набор вопросов, разделенных на группы в соответствии со структурой стандарта ISO 17799: безопасность персонала, политика безопасности, управление доступом, планирование непрерывной работы и пр. (Рисунок 1).

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

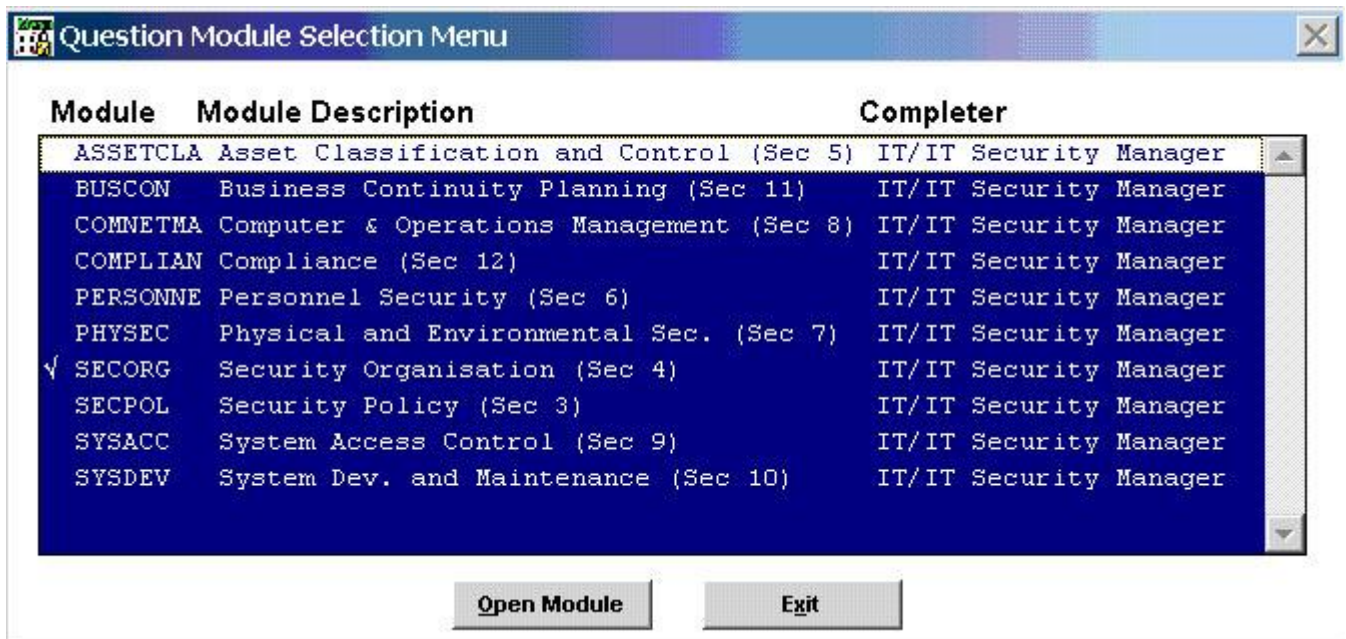


Рисунок 1 – Группы вопросов для анализа состояния ИБ системой «COBRA»

На основе введенной таким образом информации может быть получен отчет о состоянии информационной безопасности и степени ее соответствия требованиям стандарта. В частности, такой отчет может состоять из пяти основных разделов:

- 1) Вводная часть.
- 2) Перечень основных направлений работы, подвергнутых проверке.
- 3) Оценка уровня несоответствий
- 4) Перечень организационных мероприятий, реализация которых необходима для выполнения требований стандарта.
- 5) Перечень заданных вопросов и данных на них ответов.

Помимо текстовой части, в отчет также могут быть включены графики, наглядно отражающие уровни выполнения требований стандарта (Рисунок 2).

Дополнительные модули, входящие в полную версию программного продукта, необходимы для обеспечения более полного и гибкого анализа рисков в условиях конкретного предприятия.

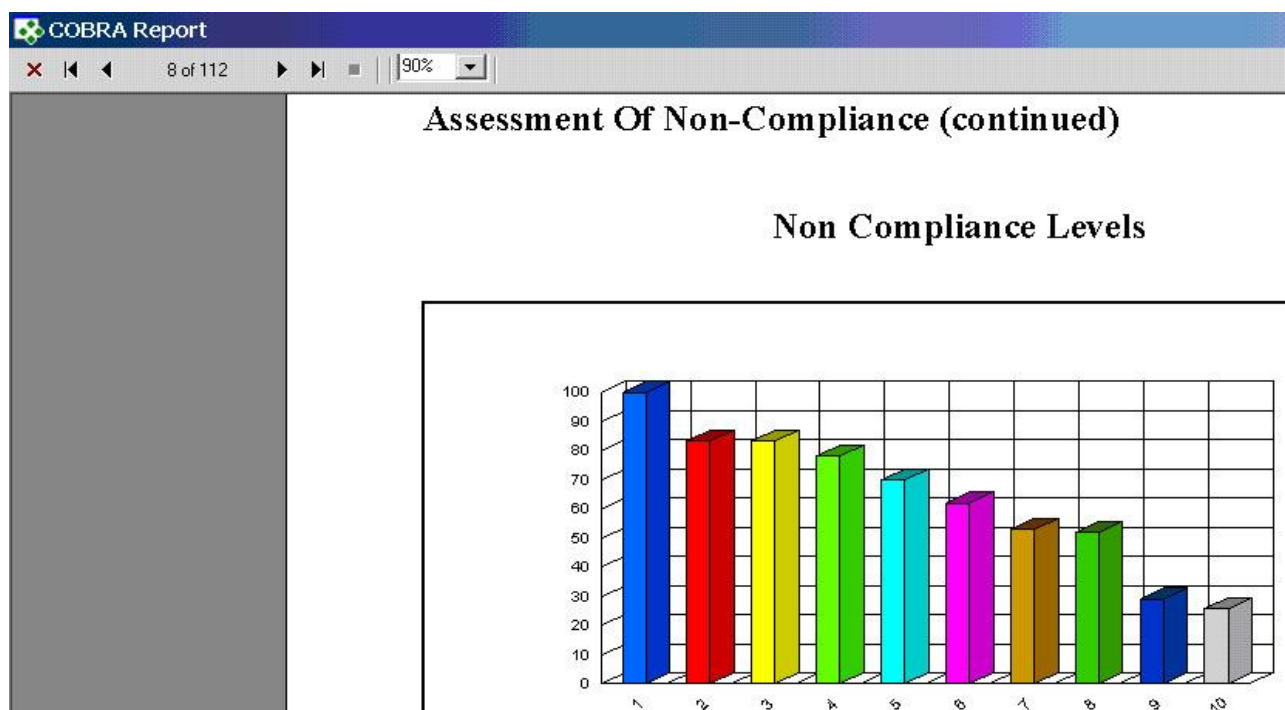


Рисунок 2 – График выполнения требований стандарта

The screenshot displays the 'COBRA Report' interface. The main title is 'Improvements Required (continued)'. Below it, the 'Risk Category' is 'System Access Control'. A table lists the required improvements, with columns for 'NUMBER' and 'TEXT'.

NUMBER	TEXT
71	Business requirements for access control should be defined and documented. (9.1.1)
72	There should be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services. Access to multi-user information services should be controlled through a formal user registration process. (9.2.1)
73	The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application controls) should be restricted and controlled. (9.2.2)

Рисунок 3 – Раздел отчета о состоянии информационной безопасности

К числу программных продуктов такого рода, аналогичных британской системе «COBRA», относится также «Программный комплекс управления политикой информационной безопасности компании КОНДОР+», поставляемый Санкт-Петербургской фирмой «Диджитал Секьюрити». Он содержит как электронные справочники, так и *модуль*, осуществляющий интерактивное взаимодействие с пользователем в процессе анализа и совершенствования политики информационной безопасности. Данный программный комплекс, помимо сборника типовых политик безопасности, включает в себя четыре основных функциональных модуля (раздела):

1) «Проект» – предназначен для сбора информации о состоянии информационной безопасности.

2) «Отчеты» – предназначен для детального анализа состояния информационной безопасности на основе введенных данных.

3) «Диаграммы/статистика» – предназначен для сводного анализа состояния информационной безопасности.

4) «Анализ рисков» – предназначен для количественной оценки существующих рисков.

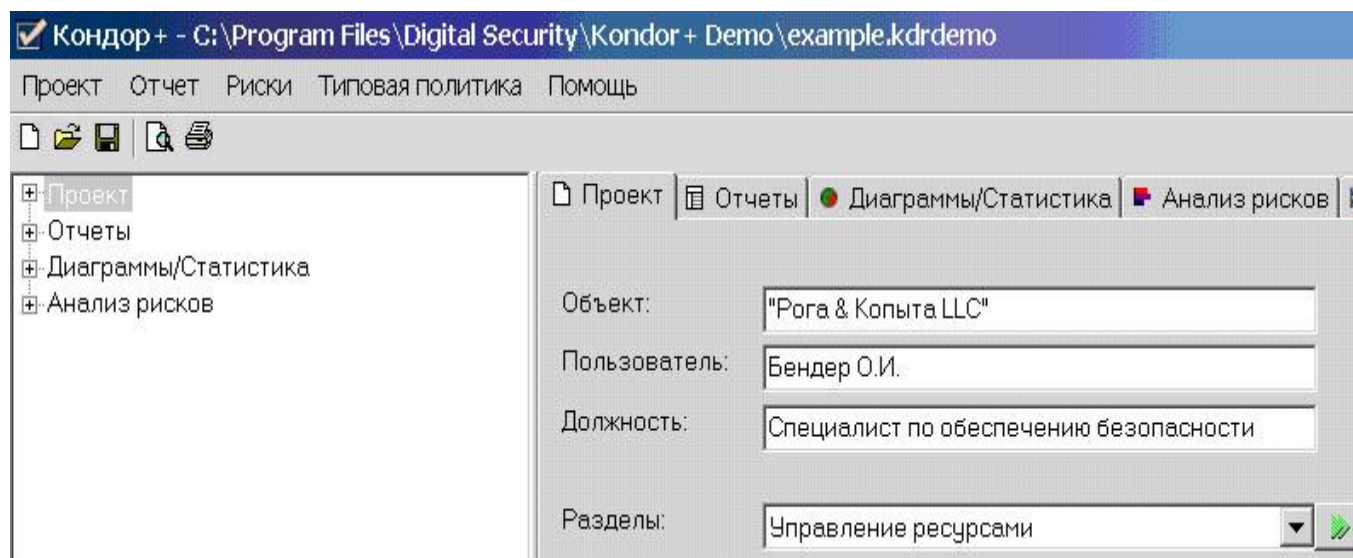


Рисунок 4 – Основные модули «Программного комплекса КОНДОР+»

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Кондор+ - C:\Program Files\Digital Security\Kondor+ Demo\example.kdrdemo

Проект Отчет Риски Типовая политика Помощь

Проект

- Политика безопасности (0/10)
- Организационные меры (15/15)
 - Существуют ли в компании форумы
 - Какие вопросы, связанные с поли
 - Существуют ли в компании форумы
 - Рассматривается ли на этом фору
 - Рассматривается ли на этом фору
 - Является ли одной из поставлен
 - Рассматривается ли на этом фору
 - Рассматривается ли на этом фору
 - Проводится ли на этом форуме в
 - Существует ли в ИС распределен
 - Определены ли ресурсы по кажды

Проект | Отчеты | Диаграммы/Статистика | Анализ рисков | Демо-версия

Существуют ли в компании форумы по координации вопросов, связанных с обеспечением информационной безопасности?

☐ Да

☒ Нет

Рисунок 5 – Модуль «Проект» – ответы на вопросы о состоянии ИБ

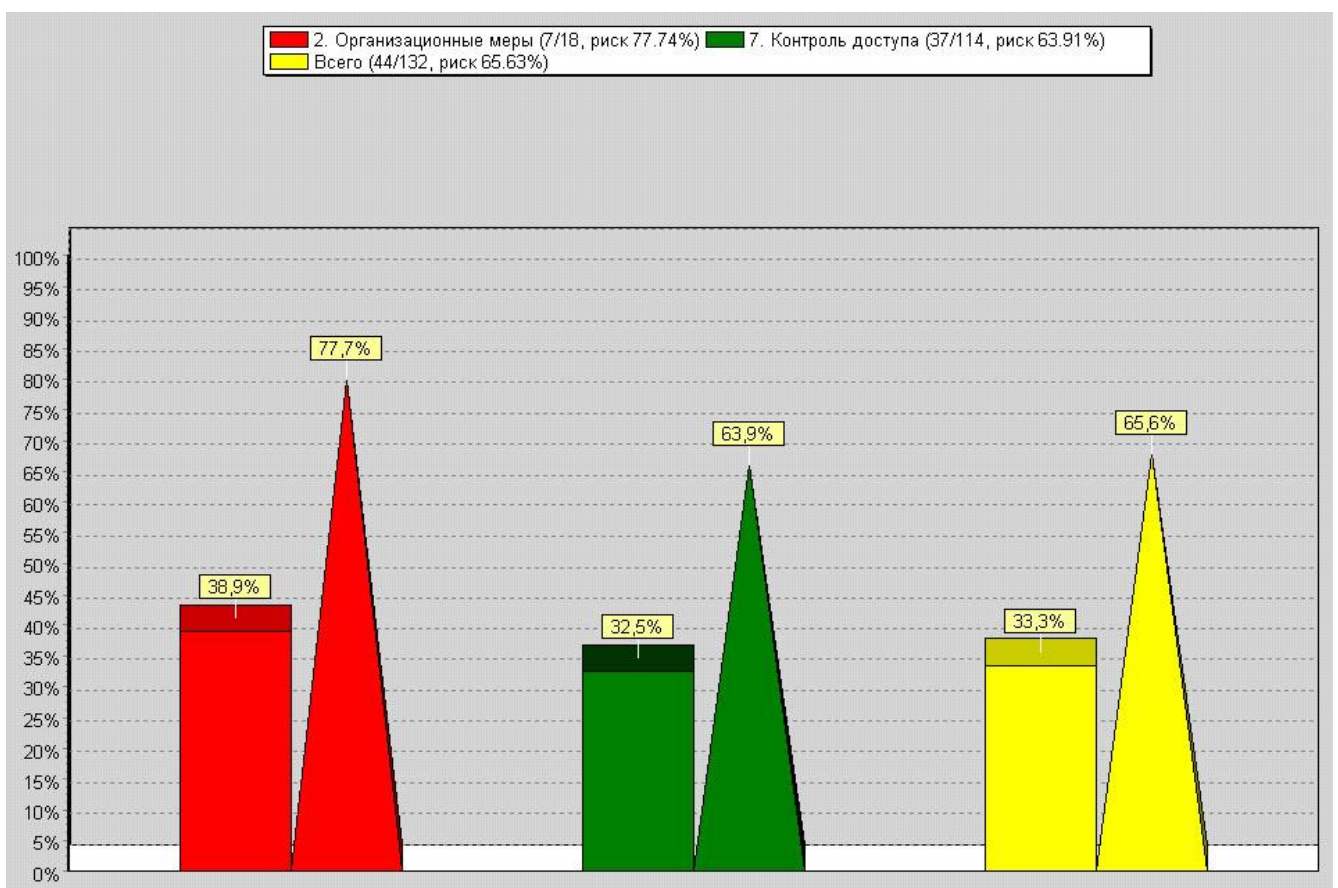


Рисунок 6 – Графическое представление сводных данных об имеющихся несоответствиях

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Так же, как и в системе «COBRA», в модуле «Проект» «Программного комплекса КОНДОР+» пользователю – ответственному менеджеру – предлагается ответить на вопросы, сгруппированные в соответствии со структурой стандарта ISO 17799 и имеющие определенные варианты ответов.

На основе введенной таким образом информации программа автоматически формирует как сводную статистику, представляемую в виде диаграмм для каждого раздела стандарта ISO 17799, так и детализированные отчеты об имеющихся несоответствиях.

При анализе несоответствий в модуле «Отчеты» пользователь имеет возможность при помощи справочной подсистемы обратиться к комментариям и рекомендациям экспертов, описывающим отдельные вопросы практического применения стандарта ISO 17799.

Таким образом, программный комплекс «КОНДОР+» позволяет провести весь комплекс работ по сбору сведений о состоянии информационной безопасности и организации защитных мер на предприятии, сопоставлению фактического положения дел с требованиями стандарта ISO 17799 (как укрупненно, так и детально) и определению приоритетных направлений дальнейшего развития системы менеджмента.

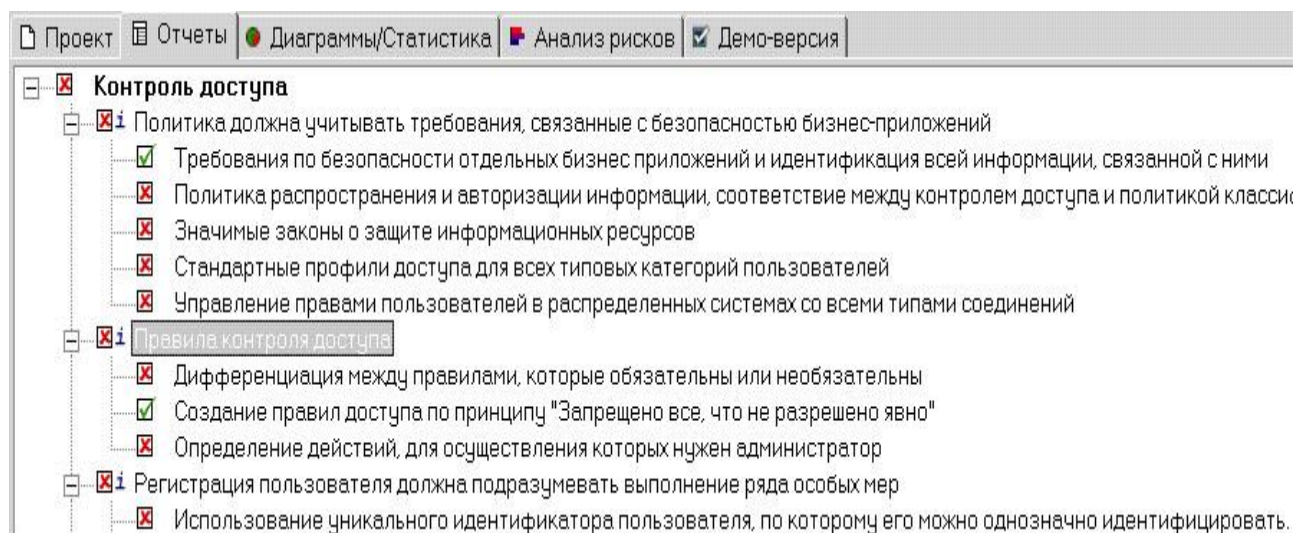


Рисунок 7 – Графическое представление сводных данных об имеющихся несоответствиях

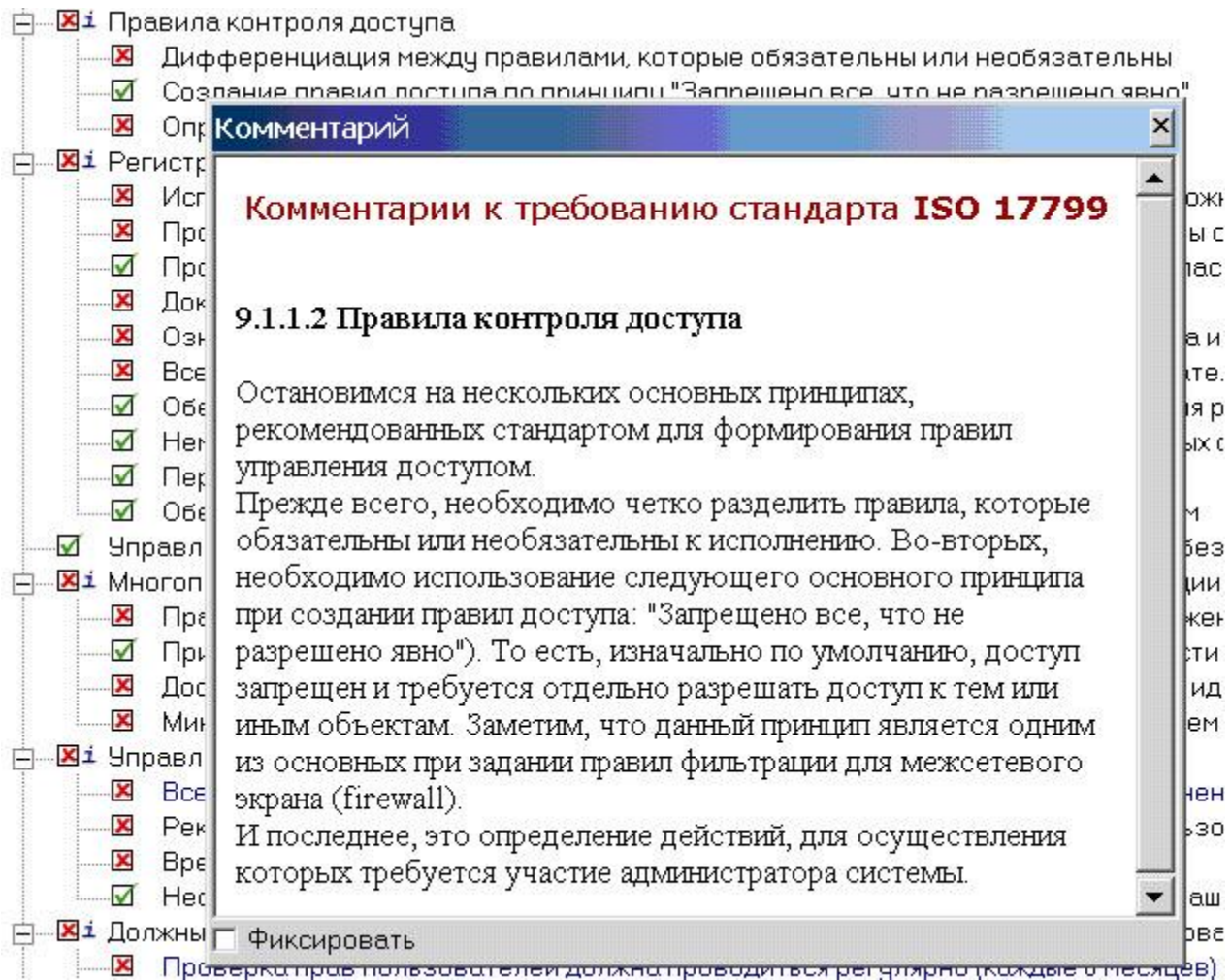


Рисунок 8 – Вызов экспертного комментария по определенному вопросу

3 Программная поддержка анализа рисков

Анализ рисков для информационной безопасности (как количественный, так и качественный), представляет собой одну из наиболее сложных задач в общей системе организационной и аналитической работы. Методологии анализа рисков и программные средства, реализующие эти методологии, как правило, предполагают выполнение следующих основных шагов, необходимых для формирования комплексной оценки существующих рисков:

- сбор информации об объектах защиты;
- выявление и оценка возможных угроз и уязвимостей;
- формирование сводной оценки рисков.

В большинстве случаев конечной целью такого анализа является формализованная оценка потребности предприятия в безопасности и

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

определение основных приоритетов развития системы защиты информации, а также создание информационной базы для оценки экономической эффективности вложений в реализацию отдельных мероприятий по обеспечению информационной безопасности.

Одним из инструментальных средств анализа рисков является семейство программных продуктов «CRAMM», поставляемых британской компанией «Insight Consulting»: «CRAMM Expert» и «CRAMM Express». Данный программный пакет основан на одноименной методике анализа рисков (CCTA Risk Analysis and Management Method – CRAMM), разработанной в 1985-1987 годах Центральным агентством по компьютерам и телекоммуникациям (Central Computer and Telecommunications Agency – CCTA) Великобритании и в дальнейшем переданной в ведение Службы безопасности Великобритании. Первую коммерческую версию программного продукта, который автоматизирует аналитические процедуры, осуществляемые в соответствии с методом CRAMM, CCTA выпустила в 1988 году, а его четвертая версия была выпущена в 2001 году уже компанией Insight Consulting.

Использование системы CRAMM включает в себя несколько последовательных этапов:

- изучение всех элементов анализируемой информационной системы;
- оценка угроз для информационной системы;
- сводный анализ рисков; принятие мер к устранению выявленных недостатков (Рисунок 9).

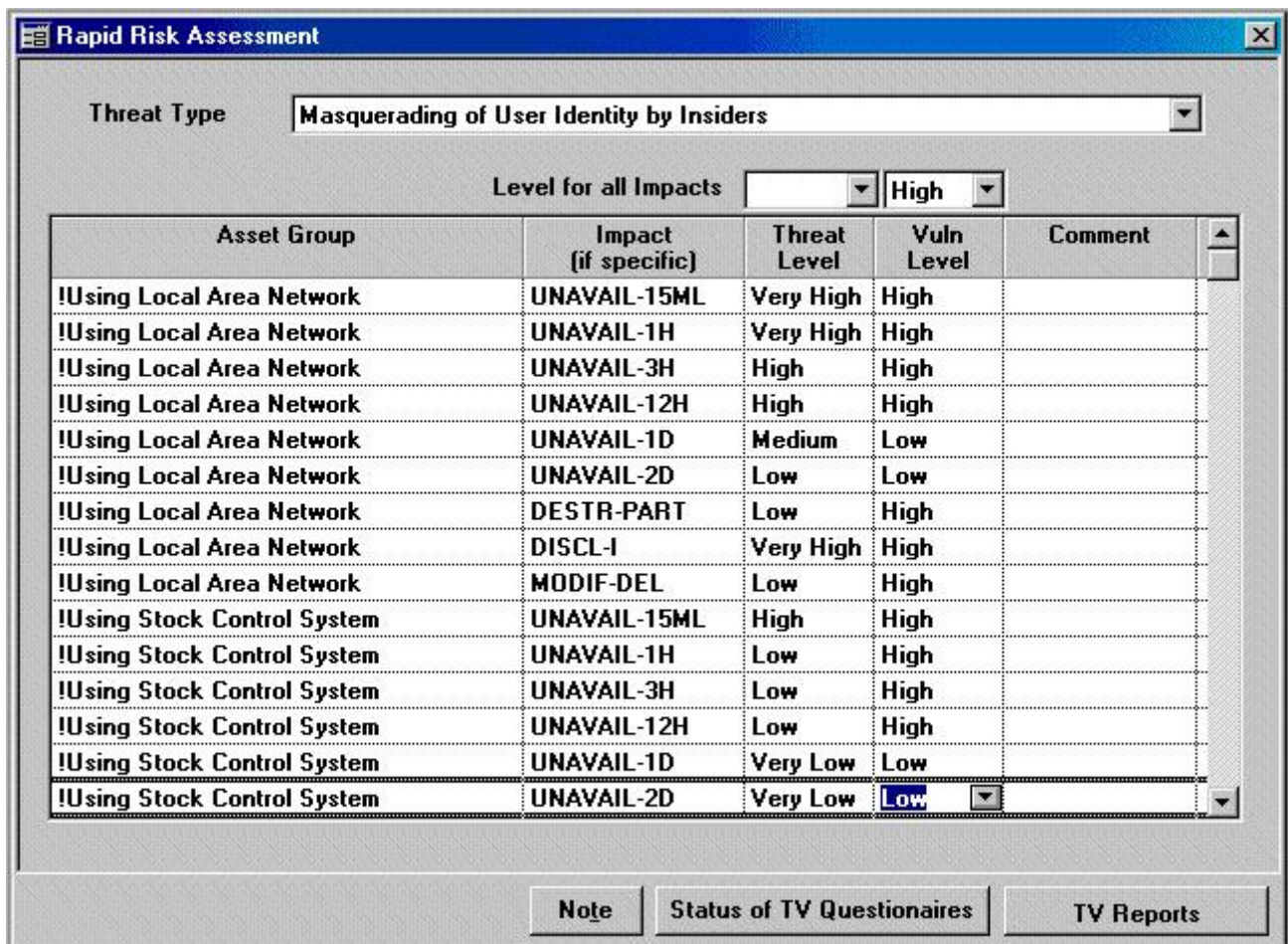
Тема 2.8 – Программные средства планирования и управления информационной безопасностью

(Планирование и управление информационной безопасностью)



Рисунок 9 – Схема применения системы CRAMM

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)



Rapid Risk Assessment

Threat Type: **Masquerading of User Identity by Insiders**

Level for all Impacts: **High**

Asset Group	Impact (if specific)	Threat Level	Vuln Level	Comment
!Using Local Area Network	UNAVAIL-15ML	Very High	High	
!Using Local Area Network	UNAVAIL-1H	Very High	High	
!Using Local Area Network	UNAVAIL-3H	High	High	
!Using Local Area Network	UNAVAIL-12H	High	High	
!Using Local Area Network	UNAVAIL-1D	Medium	Low	
!Using Local Area Network	UNAVAIL-2D	Low	Low	
!Using Local Area Network	DESTR-PART	Low	High	
!Using Local Area Network	DISCL-I	Very High	High	
!Using Local Area Network	MODIF-DEL	Low	High	
!Using Stock Control System	UNAVAIL-15ML	High	High	
!Using Stock Control System	UNAVAIL-1H	Low	High	
!Using Stock Control System	UNAVAIL-3H	Low	High	
!Using Stock Control System	UNAVAIL-12H	Low	High	
!Using Stock Control System	UNAVAIL-1D	Very Low	Low	
!Using Stock Control System	UNAVAIL-2D	Very Low	Low	

Note Status of TV Questionnaires TV Reports

Рисунок 10 – Оценка взаимосвязей между различными угрозами и информационными сервисами в системе CRAMM

На основе всех введенных данных и по результатам расчетов и обработки информации могут быть получены сводные характеристики уровней риска для анализируемой информационной системы и, в частности, для отдельных информационных сервисов (Рисунок 11).

После того как произведена оценка рисков, система предлагает реализовать конкретные меры по повышению уровня защищенности, используя введенную информацию о состоянии информационной безопасности, а также собственную «Библиотеку контрмер» – базу знаний, которая содержит примеры и рекомендации (как конкретные, так и общие), относящиеся к различным аспектам защиты информационных ресурсов. С их применением может быть начат переход от анализа рисков к непосредственным управленческим действиям по обеспечению информационной безопасности:

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

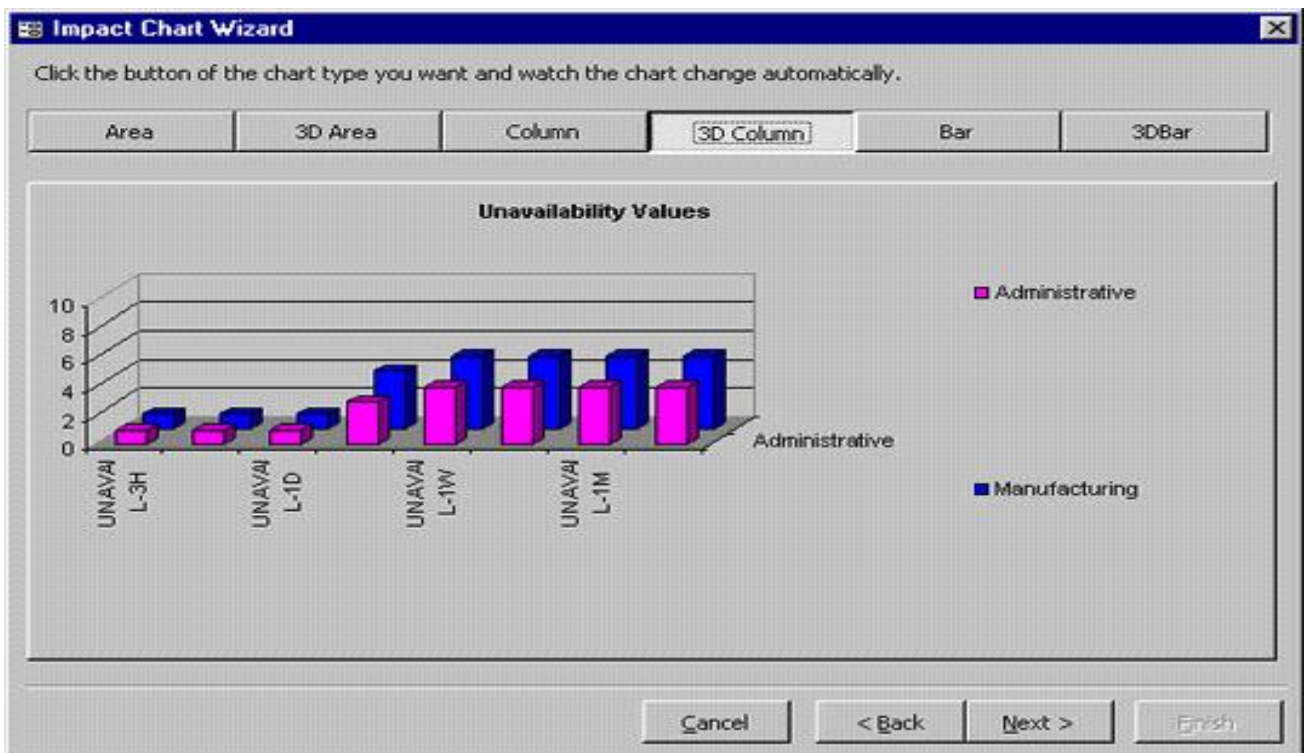


Рисунок 11 – Пример сводной оценки рисков недоступности двух информационных подсистем

- разработка мероприятий по противодействию угрозам (Рисунок 12);
- совершенствование системы реагирования на инциденты;
- устранение несоответствий требованиям стандарта ISO 17799 и других нормативных документов (Рисунок 13).



Рисунок 12 – Дерево контрмер системы CRAMM

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

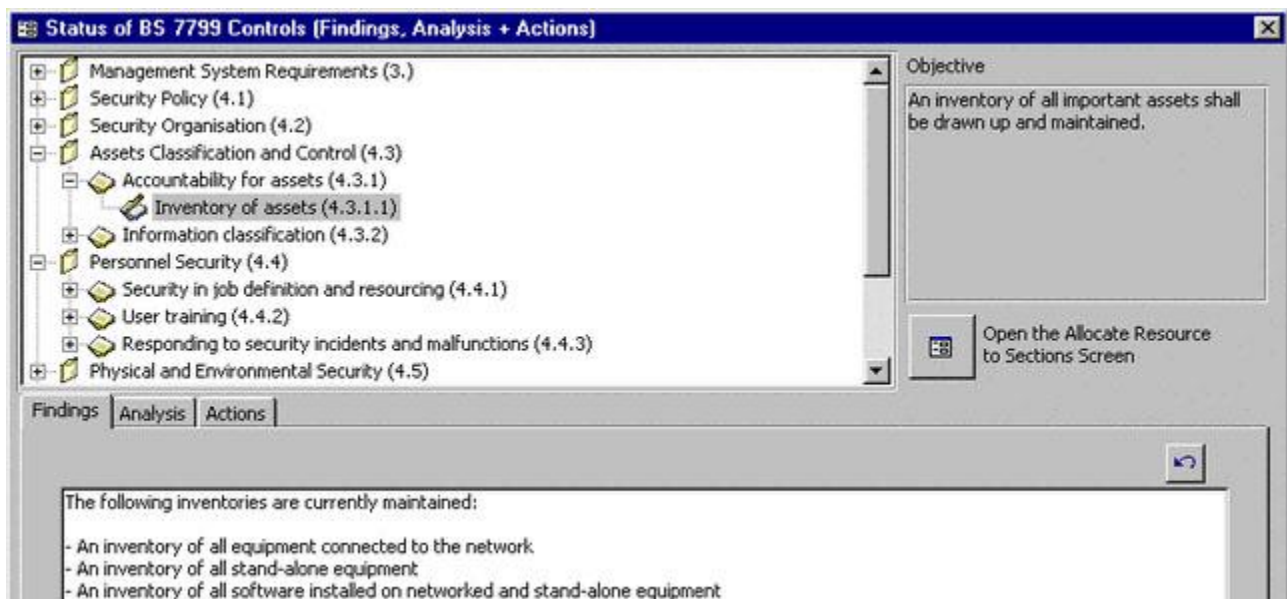


Рисунок 13 – Окно анализа несоответствий требованиям стандарта ISO17799/BS7799

Таким образом, в результате использования всех перечисленных инструментов системы CRAMM предприятие может осуществить комплекс работ по управлению информационной безопасностью и создать не только хорошо контролируемую систему защиты информации, но и информационную базу, позволяющую в будущем оценить целесообразность вложений в реализацию дополнительных мероприятий по обеспечению информационной безопасности и инвестиций в отдельные средства защиты информации.

4 Программные средства, интегрируемые в информационную систему предприятия

Еще одним направлением развития программных средств, обеспечивающих поддержку организационной работы в сфере информационной безопасности, является создание и внедрение комплексных средств анализа поведения пользователей в информационной системе. Во многом такие функции и используемые алгоритмы схожи с функциями и алгоритмами средств обнаружения вторжений. Основные функции таких программных средств:

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

- проверка действий пользователей на их соответствие действующим политикам безопасности;
- выявление нарушений действующей политики информационной безопасности;
- установление лиц, чьи действия приводят к нарушениям и создают угрозы информационной безопасности.

Основными функциями, реализуемыми программным обеспечением такого типа, являются сбор первичных данных о действиях пользователей, их автоматизированный анализ с учетом требований политики безопасности и осуществление необходимых активных действий: информирование администраторов, временное ограничение прав пользователей и пр.

Один из программных продуктов такого типа – «INSIDER – Система обнаружения внутреннего нарушителя», поставляемая российской компанией «Праймтек». Эта система накапливает сведения о поведении пользователей, а также позволяет инициировать определенные активные действия (например, для предотвращения выявленного длящегося нарушения).

В частности, для анализа поведения пользователей в информационной системе могут быть использованы следующие данные:

- показатели интенсивности использования различных пользовательских приложений;
- показатели интенсивности (частоты, объема) чтения, копирования и удаления файлов;
- показатели интенсивности отправки и приема электронных сообщений;
- показатели интенсивности передачи данных по сети;
- попытки подбора паролей;
- действия с системными файлами и реестром;
- действия с системными утилитами и пр.

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Таким образом, у администраторов информационных систем, специалистов по информационной безопасности и руководителей предприятия появляются возможности для реагирования на инциденты, пресечения потенциально опасных действий и выявления нарушителей из числа персонала предприятия.

Также среди информационных платформ, интегрируемых в информационную систему предприятия и специально предназначенных для реализации и контроля выполнения политик безопасности, выделяются такие продукты, как:

- 1) Tivoli Security Information and Event Manager компании IBM, а также комплекс смежных продуктов, относящихся к т.н. IBM security framework
- 2) MARS: Security Monitoring, Analysis, and Response System компании Cisco.

Tivoli Security Information and Event Manager включает в себя:

- A) Tivoli Security Operations Manager.
- Б) Tivoli Compliance Insight Manager.

Tivoli Compliance Insight Manager представляет собой специальную программную платформу, которая обеспечивает контроль выполнения требований политики безопасности, а также автоматизирует значительную часть работы при проведении аудитов информационной безопасности и анализе защищенности данных. В частности, данное ПО обеспечивает сбор, анализ и защищенное хранение журналов (логов) работы различных приложений, операционных систем и платформ и их интерпретацию в терминах, понятных нетехническим специалистам. Таким образом, отчеты, формируемые данной системой, могут быть понятны бизнес-менеджерам и аудиторам и использованы для контроля выполнения требований политик безопасности.

Tivoli Security Operations Manager предназначен для контроля событий в корпоративной информационной системе и выявления нарушений и подозрительных действий в режиме близком к режиму реального времени.

Тема 2.8 – Программные средства планирования и управления информационной безопасностью
(Планирование и управление информационной безопасностью)

Система MARS также обеспечивает сбор и централизованное хранение данных о системных событиях, которые поступают от различных устройств и платформ, входящих в корпоративную информационную систему, и обеспечивает возможность централизованного оперативного контроля за соблюдением установленных требований. Также MARS интегрирован с программным комплексом Cisco Security Manager, который, в свою очередь, позволяет централизованно и унифицированно управлять настройками безопасности в различных системах защиты и системах обнаружения вторжений, установленных в компании.