УДК 681.3.06:519.248.681

Л. В. СКРИПНИК, , д-р техн. наук, М. Ф. БОНДАРЕНКО, д-р техн. наук,
И. Д. ГОРБЕНКО, д-р техн. наук, , А. А. ТКАЧ, А.В. ПОТИЙ, канд.техн. наук

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ГЕРМАНСКОГО СТАНДАРТА «РУКОВОДСТВО ПО БАЗОВОЙ ЗАЩИТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Введение

Одной из актуальнейших задач обеспечения безопасности информационных систем различного класса и назначения является формирование отечественной нормативной и методологической базы. В настоящее время в Украине идет разработка отечественной нормативной базы по защите информации в различных информационных технологиях (ИТ), автоматизированных системах управления (АСУ), компьютерных системах и сетях (КСС) и др. Обзору существующих современных международных стандартов была посвящена статья [1]. Определенным прорывом в области проектирования, изготовления, оценки (сертификации) и эксплуатации защищенных информационных технологий стало принятие международного стандарта ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий» [2]. Ряд государств мира принимают или рассматривают его с целью принятия в качестве национального методом «обложки». Среди технически развитых государств, которые разработали национальные стандарты обеспечения информационной безопасности, необходимо, прежде всего, выделить Германию, в частности «Руководство по базовой защите информационных технологий» [3], принятое в качестве стандарта Германии.

Цель настоящей статьи является рассмотрение основных методологических положений германского стандарта «Руководство по базовой защите информационных технологий» (далее – Руководство), который разработан Германским информационным агентством безопасности (BSI).

Центральная идея разработчиков Руководства заключается в оказании помощи пользователям и владельцам информационных технологий в оперативном решении общих задач информационной безопасности, повышении уровня защиты ИТ и ИТ-систем , а также упрощения процессов создания политики и концепции безопасности ИТ. Это достигается посредством предоставления определенных наборов стандартных защитных мероприятий безопасности, рекомендаций и средств по реализации для типичных систем ИТ.

Под понятием «базовой защиты информационной технологии» в данном документе понимается некоторый обоснованный в пределах разумного уровень защиты для ИТ, адекватный нормальным требованиям защиты, который в тоже время может служить базисом для ИТ-систем и ИТ-приложений, требующих более высокую степень защиты. Это обеспечивается через соответствующее применение организационных, кадровых, инфраструктурных и технических стандартных защитных мер безопасности. Следует попутно отметить, что понятия «разумный уровень защиты» и «нормальные требования защиты» в Руководстве не определены и скорее интуитивно понимается пользователями, точнее разработчиками документа, т.к. последний регулярно модифицируется и расширяется.

Под стандартными защитными мерами безопасности в Руководстве понимается некоторая совокупность идентифицированных мероприятий безопасности, являющихся общими для групп «типичных» ИТ-систем.

Под группами «типичных» ИТ-систем понимаются специфические группы активов (assets) информационных технологий, которые в большинстве неспециализированных ИТ можно выделить как «типичные», то есть являющихся широко распространенными (не индивидуальными)

решениями и характеризующиеся обычными требованиями защиты в отношении конфиденциальности, целостности и доступности.

Активы (assets) информационной технологии включают не только ресурсы самой компьютерной системы, но и организационную, кадровую и инженерно-строительную инфраструктуры, обеспечивающие и поддерживающие её функционирование.

1. Структура документа

Концептуальный подход Руководства заключается в том, что обеспечение безопасности информационной технологии должно носить комплексный характер, т.е. необходимый уровень ИТ-безопасности должен достигаться не только реализацией стандартных защитных мер непосредственно в технических компонентах (отдельных продуктах информационной технологии), но также и реализацией мероприятий, охватывающих аспекты организационной, кадровой и инженерно-строительной инфраструктур.

Чтобы облегчить структурирование и обработку высоко гетерогенных областей ИТ, включая операционные среды, Руководство базовой защиты ИТ построено по модульному принципу. Отдельные модули отражают типичные области использования ИТ-активов, например сети клиент/сервер, здания, связь, прикладные компоненты и т.д.

Руководство базовой защиты ИТ состоит из следующих разделов.

Раздел «Введение и процедура» (главы 1 и 2) определяет концепцию базовой защиты ИТ, содержит указания по использованию Руководства и описывает процедуру составления концепции безопасности, которая позволяет представить базовую защиту ИТ.

Второй раздел Руководства (главы 3- 9) содержит отдельные (унифицированные) структурные модули для различных ИТ-компонентов, процедур и ИТ-систем. Модули сгруппированы в следующие главы:

Глава 3: Базовая защита универсальных ИТ-компонентов;
Глава 4: Инфраструктура;
Глава 5: Системы с несетевой структурой;
Глава 6: Системы с сетевой структурой;
Глава 7: Системы передачи данных;
Глава 8: Передача данных;
Глава 9: Другие ИТ-компоненты.

Раздел «Каталоги угроз» содержит детальные описания угроз, которые включены в сценарии угрозы для индивидуальных модулей. Угрозы сгруппированы в пять каталогов:

T1: Форс-мажор;
T2: Организационные недостатки;
T3: Ошибка оператора;
T4: Технический отказ;
T5: Преднамеренные действия.

Раздел «Каталоги защитных мер» содержит детальные описания стандартных защитных мер безопасности ИТ, упомянутых в различных модулях Руководства. Мероприятия сгруппированы в шесть каталогов мер безопасности:

S 1: Меры защиты инфраструктуры;
S 2: Организационные меры защиты;
S 3: Меры безопасности персонала, в смысле безопасности персонала для активов;
S 4: Меры защиты аппаратных средств и программного обеспечения;
S 5: Меры защиты связи;
S 6: Планирование мер безопасности для нештатных ситуаций (непредвиденных обстоятельств).

Последний раздел «Приложения» Руководства содержит вспомогательные средства, формы, краткие описания инструментальных средств, охватывающих все положения базовой защиты ИТ и списка зарегистрированных пользователей справочника.

В свою очередь каждый отдельный (унифицированный) структурный модуль включает сценарии угроз для типичных областей использования ИТ-активов и рекомендуемый набор стандартных мер защиты. «Сценарий угрозы» обеспечивает базис для формирования определенного набора стандартных мер защиты, путем из соответствующих каталогов S 1, S 2, S 3, S 4, S 5, S 6 Каталога защитных мер. Они разработаны с точки зрения пользователя ИТ и приведены для лучшего понимания и в дальнейшем не требуются пользователю для создания концепции безопасности,

Для каждого отдельного (унифицированного) структурного модуля связь между угрозами и рекомендуемыми защитными мерами безопасности показывается в таблице «Угрозы – защитные меры безопасности». Как пример, ниже в табл. 1 приведена выборка из Руководства таблицы «Угрозы – защитные меры безопасности» для модуля «Обмен данными средств информации».

Таблица 1

	Приоритет	Т 1. 7	Т 1. 8	Т 1. 9	Т 2. 3	Т 2. 10	Т 2. 17	Т 2. 18	Т 2. 19	Т 3. 1	Т 3. 3	Т 3. 12	Т 3. 13	Т 4. 7	Т 5. 1	Т 5. 2	Т 5. 4	Т 5. 9	Т 5. 23	Т 5. 29	Т 5. 43
S 1.36	2*	X	X							X					X	X	X	X		X	
S 2.3	2				X	X	X							X	X	X	X	X	X	X	X
S 2.42	2							X		X											
S 2.43	1					X	X	X				X									
S 2.44	1	X	X	X								X		X	X	X		X		X	

Заголовки столбцы показывают угрозы, перечисленные в модуле. Крайний левый столбец показывает номера защитных мер безопасности. Столбец 2 показывает приоритет, назначенный для данной защитной меры безопасности. Если этот столбец содержит звездочку, то соответствующая мера безопасности рассматривается как "необязательная" в этом модуле. Другие столбцы показывают зависимость между защитными мерами безопасности и угрозами. Символ "X" в данной клетке показывает, что соответствующая защитная мера безопасности эффективна против соответствующей угрозы. Эффект меры безопасности может быть или профилактической природы иначе нацелен на смягчение потери или повреждения. Отсутствие символа "X" в каком-либо столбце говорит о том, что против данной угрозы отсутствует защитные меры безопасности.

2. Применяемые критерии определения и оценки уровня безопасности ИТ

В отличие от традиционного подхода к анализу риска, подход, принятый в Руководстве базовой защиты ИТ, требует только, чтобы было выполнено целевое сравнение, путем реального сопоставления, между рекомендуемыми и уже осуществленными мероприятиями. Для определения и оценки уровня безопасности ИТ используется модель базовой защиты активов ИТ, которая составлена из различных унифицированных модулей глав 3 – 9 Руководства и отображает существенные аспекты безопасности активов ИТ на определенные модули и наоборот. Критерием является степень соответствия совокупности реализованных мер защиты активов ИТ стандартным защитным мероприятиям из соответствующих унифицированных модулей модели базовой защиты активов ИТ, которая используется как испытательный план. Недостатки безопасности, которые должны быть устранены посредством принятия рекомендуемого мероприятия, определены в терминах того идентифицированного мероприятия безопасности, которое отсут-

ствует или еще не осуществлено. Только в случаях, когда требование защиты ИТ значительно выше, необходимо также выполнить дополнительный анализ безопасности, взвешивая рентабельность осуществления дополнительного мероприятия.

Руководство базовой защиты ИТ определяет качественные формулировки при назначении требований защиты по трем категориям.

- базовая умеренная - воздействие любой грозы или ущерба ограничено;
- высокая - воздействие любой угрозы или ущерба может быть значительно;
- очень высокая - воздействие любого ущерба может достигать катастрофических размеров, которые могли угрожать самому выживанию агентства/компании.

Также Руководство содержит следующие рекомендации относительно категорий требований защиты, обеспечиваемых стандартными защитными мерами безопасности (табл. 2).

Таблица 2

Категория требований защиты	Защитный эффект стандартных защитных мер безопасности, нацеленных на достижение базовой защиты ИТ
Базовая умеренная	Стандартные защитные меры безопасности, нацеленные на базовую защиту ИТ, в целом адекватны и разумны.
Высокая	Стандартные защитные меры безопасности, нацеленные на базовую защиту ИТ, предоставляют базовый уровень защиты, но могут быть недостаточными. Дополнительные защитные меры могут быть установлены, выполняя дополнительный анализ безопасности.
Очень высокая	Стандартные защитные меры безопасности, нацеленные на базовую защиту ИТ, предоставляют базовый уровень защиты, но в общем недостаточны. Необходимые дополнительные защитные меры безопасности должны быть установлены на разовом базисе на основе дополнительного анализа безопасности.

Оценка требований защиты проводится последовательно для приложений, систем, линий связи и помещений ИТ. Цель оценки требований защиты состоит в определении требуемой степени защиты в терминах конфиденциальности, целостности и доступности.

3. Рекомендации по методологии и практических средствах реализации

Модульная структура Руководства предоставляет пользователям возможность просто и экономно формировать и осуществлять концепции безопасности ИТ в терминах требуемых ресурсов. Для достижения среднего уровня защиты достаточно идентифицировать модули, существенные для рассматриваемой системы или активов ИТ, и осуществить все защитные меры, рекомендуемые в тех модулях непротиворечивым способом. Руководство определяет, что эффективная реализация защитных мер безопасности ИТ требует хорошо обдуманного и управляемого процесса безопасности ИТ. Для обеспечения соответствующего уровня безопасности ИТ функциональное управление защитой ИТ в обязательном порядке должно быть организовано в начале процесса безопасности ИТ и интегрировано в существующие структуры организации. Для обеспечения непрерывного и эффективного процесса безопасности ИТ Руководство базовой защиты ИТ содержит рекомендации по методологии и практических средствах реализации. Оно также содержит возможные решения к различным задачам, касающимся безопасности ИТ, типа составления концепции безопасности ИТ, контроля средств защиты и сертификации. Различные варианты использования Руководства базовой защиты ИТ зависят от решаемых задач. Руководство определяет следующий план действий, которые являются необходимыми для поддержания непрерывного процесса безопасности ИТ:

- разработка политики безопасности ИТ;
- выбор и создание соответствующей организационной структуры для управления безопасностью ИТ;
- составление концепции безопасности ИТ;
- реализация защитных мер безопасности ИТ;
- организация обучения персонала и пользователей;
- текущее поддержание безопасности ИТ.

Процесс безопасности ИТ начинается с определения целей защиты ИТ и установления управления защитой ИТ. В состав функций управления защитой ИТ включены функции по составлению и осуществлению концепции безопасности ИТ. Этот подход иллюстрирован схематично в рис. 1.

Рис. 1

В главе 3.0 Руководства приведено описание процесса управления защитой ИТ и детальное объяснение индивидуальных действий в форме рекомендуемых стандартных защитных мер безопасности ИТ. Руководство определяет, что первичной функцией управления защитой ИТ является разработка концепции безопасности ИТ, которая является необходимой для реализации необходимых защитных мер безопасности ИТ. В частях 2.1 – 2.6 главы 2 приведено описание создания концепции безопасности ИТ, с использованием Руководства базовой защиты ИТ. Общая процедура создания концепции безопасности ИТ схематически приведена на рис. 2.

Методология анализа структуры ИТ приведена в части 2.1 главы 2 и включает следующие подзадачи:

- подготовка плана сети ИТ;
- сокращение сложности для идентификации групп подобных активов
- сбор информации о системах ИТ
- фиксация информации о приложении ИТ и связанной информации

Отправной точкой для анализа структуры ИТ служит топологический план сети ИТ, который является графическим представлением рассматриваемых компонентов, используемых в ИТ, области связи и способов их объединения в сеть. В процессе анализа структуры ИТ должны

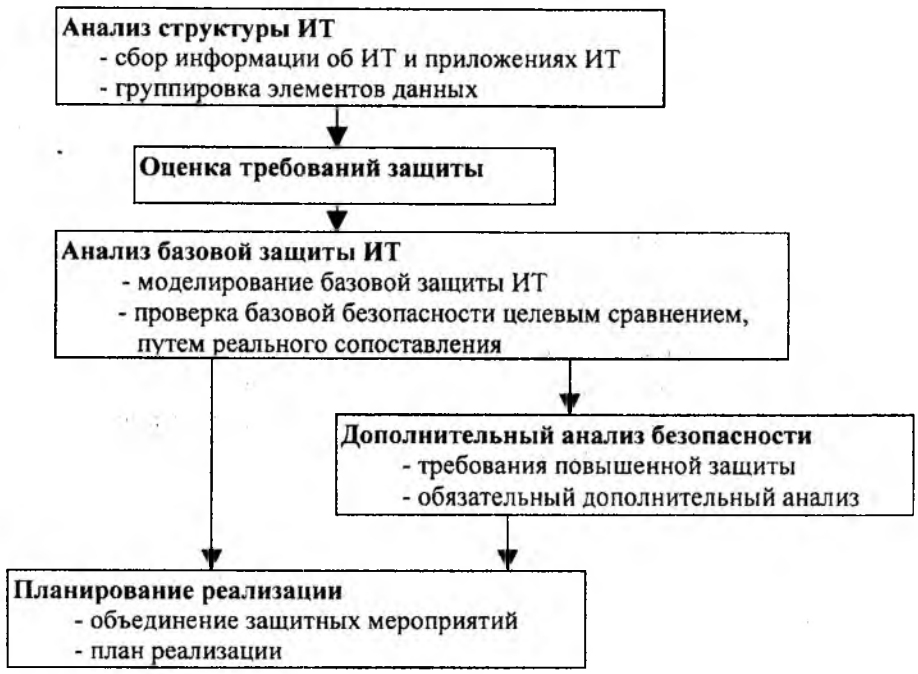

Рис. 2

быть рассмотрены:

- ·существующая инфраструктура;
- ·поддерживающее организационное и кадровое окружение активов ИТ;
- ·используемые системы ИТ (сетевые и несетевые);
- ·линии коммуникаций между системами ИТ и внешним миром;
- ·приложения ИТ, исполняемые на активах ИТ.

Руководство определяет, что план должен представлять следующие объекты:

- системы ИТ, то есть клиентские и сервер компьютеры, активные сетевые компоненты (типа центров, переключателей, маршрутизаторы), сетевые принтеры и т.д.;
- сетевые подключения между этими системами, т. е. подключения LAN (например локальная сеть на основе протокола CSMA-CD, эстафетное кольцо), базовые технологии (например. FDDI, ATM), и т.д.;
- подключения между рассматриваемой областью ИТ и внешним миром, т. е. удаленный доступ по телефону или модему, подключения Internet, использующие ISDN, модем или маршрутизаторы, радио связь или арендованные каналы и т.д.

Кроме того, для каждого из объектов, представленных в плане, должна быть записана следующая информация для каждой системы ИТ:

- уникальное название (например, полное имя хоста или номер идентификации);
- тип и функция (например, сервер базы данных для приложения X);
- поддерживающая платформа (то есть аппаратная платформа и операционная система);
- расположение (например, здание и номер комнаты);
- название ответственного администратора;
- тип сетевого подключения и сетевого адреса.

Помимо этого, не только для систем ИТ, но также и для сетевых подключений между системами и подключений к внешнему миру, должно быть приведены:

- тип соединения (например, волокно оптический кабель);
- максимальная объем передачи данных (например, 10 Mbps),
- сетевые протоколы, используемые на более низких уровнях (например, локальная сеть на основе протокола CSMA-CD, TCP/IP),
- для внешних подключений, детали внешней сети (например, Internet, название средства доступа).

Поскольку структура ИТ вообще адаптируется к определенным требованиям организации, Руководство указывает на необходимость своевременного обновления сетевого плана, для отображения текущей ситуации.

На следующем шаге анализа структуры ИТ Руководство рекомендует упростить сложность плана для идентификации групп подобных активов путем удаления любой информации, которая не нужна для решения последующего множества задач, и объединения любых идентичных компонентов в одну соответствующую группу, которая будет представлена в сетевом плане отдельным объектом. Компоненты могут быть объединены в одну и ту же группу если компоненты

- имеют тот же самый тип;
- имеют идентичные или почти идентичные конфигурации;
- присоединены к сети в тем же самым или почти тем же самым способом;
- подчинены тем же самым базовым условиям и
- используют те же самые приложения.

После того, как процесс группировки закончен, компоненты, сгруппированные вместе, показываются на сетевом плане как отдельный объект. Тип и число компонентов, представленных в каждой группе, должны быть задокументированы в виде таблицы, как показано для примера на табл. 3

Таблица 3

Номер	Описание	Платформа	Номер	Инсталляционный сайт	Состояние	Пользователь (и) / Администрация.
S1	Сервер для людских ресурсов	Windows NT Сервер	1	Бонн, R 1.01	Операционный	Людские ресурсы
S2	Первичный контроллер домена	Windows NT Сервер	1	Бонн, R 3.10	Операционный	Все пользователи ИТ
C1	Группа клиентов в HR обработке данных	Windows NT Рабочая станция	5	Бонн, R 1.02 - R 1.06	Операционный	Людские ресурсы
C2	Группа клиентов в отделе администрации	Windows NT Рабочая станция	10	Бонн, R 1.07 - R 1.16	Операционный	Отдел Администрации

Для уменьшения затрат по фиксации информации о приложениях ИТ и обрабатываемой информации Руководство рекомендует рассматривать только наиболее важные выполняющиеся или планируемые приложения ИТ, для группирования которых определены три категории:

- приложения, относительно которых необходимо, чтобы их данные/ информация и программы остались конфиденциальными (т. е. максимальное требование конфиденциальности);
- приложения, относительно которой необходимо, чтобы их данные/ информация и программы были правильными и неизменными (целостность);

– приложения, для которой только минимальное количество времени простоя может допускаться (т. е. максимальные требования доступности).

Результат этого рассмотрения - резюме какие большие приложения ИТ обрабатываются, и на каких системах ИТ. Рекомендуется, чтобы результаты были задокументированы в табличной форме.

После того, как был выполнен анализ структуры ИТ, должна быть проведена оценка требований защиты (см. рис. 2). Цель оценки требований защиты состоит в том, чтобы установить то, что защита является адекватной и разумной для информации и использованного актива ИТ. Она проводится в соответствии с методическими указаниями части 2.2. главы 2 Руководства, согласно которым оценка требования защиты зафиксированной структуры ИТ осуществляется последовательным выполнением четырех отдельных шагов.

Прежде всего, должны быть определены категории требований защиты для различных приложений ИТ. Для определения требований защиты для различных приложений ИТ рекомендуется использовать типичные сценарии ущерба. По результатам определения требований защиты для различных приложений ИТ определяются требования защиты для систем ИТ. Они в свою очередь используются, чтобы определить требования защиты для маршрутов передачи и для помещений, в которых расположены активы ИТ. Оценка требований защиты для приложений ИТ проводится для каждого приложения, включая содержащиеся или используемые в нем данные. Цель оценки требований защиты состоит в определении требуемой степени защиты в терминах конфиденциальности, целостности и доступности. Категории требований защиты для приложений ИТ определяются в Руководстве через следующие сценарии ущерба:

– нарушение законов, устава или контрактов,
– ухудшение информационного самоопределения,
– физический ущерб,
– уменьшенная эффективность режимов работы,
– отрицательные эффекты на внешние отношения и
– финансовые последствия.

Часто отдельный случай потери или ущерба может включать несколько категорий ущерба. Например, отказ приложения ИТ мог мешать выполнению основной работы, заканчивающийся прямой финансовой потерей и в то же самое время потерей имиджа.

Для получения четких границ между категориями требования защиты «базовая умеренная», «высокая» и «очень высокая», верхние и нижние пределы рекомендуется определять для индивидуальных сценариев ущерба. Чтобы получить грубое представление относительно того, какое требование защиты является соответствующим данному уровню потенциального ущерба и его воздействия, можно воспользоваться соответствующими таблицами из части 2.1. Руководство допускает в отдельных конкретных ИТ наличие сценариев ущерба отличных от вышеперечисленных. В таких случаях соответствующие таблицы из части 2.1. должны быть дополнены. Каждый из сценариев ущерба рассматривается с позиции потери конфиденциальности, целостности и доступности на основе вопроса: «Что если ...?». Чтобы упростить определение возможного ущерба, в Руководстве приведен, как справочный, набор вопросов для каждого из упомянутых сценариев ущерба, как инструмент разработки сценариев ущерба. Рекомендуемый набор вопросов на является исчерпывающим, и в каждом случае необходимо рассмотреть ситуацию в определенной организации, и включить свои вопросы в дополнение к приведенным в этом Руководстве. Пример определения категории требований защиты приложений ИТ через сценарии ущерба приведен в табл. 4.

Таблица 4

Категория требования Защиты " Базовая умеренная "	
1. Нарушение законов, устава или контрактов	• Нарушения устава и законов с незначительными последствиями • Незначительные нарушения контракта, которые приводят к небольшим договорным штрафамв
2. Ухудшение права на информационное самоопределение	• Ухудшение права на информационное самоопределение было бы оценено как терпимое. • Возможное неправильное употребление персональных данных имеют минимальные эффекты на социальное или финансовое положение, тех кого касались.
3. Физический ущерб	• Не кажется возможным.
4. уменьшенная эффективность режимов работы	• Ухудшение было бы оценено как терпимое. • Максимальное приемлемое время простоя большее чем 24 часа.
5. Отрицательные эффекты на внешние отношения	• Минимальное ухудшение репутации / доверие, ограниченное в пределах агентства/предприятия.
6. Финансовые последствия	• Финансовая потеря приемлема для агентства/компании.

Оцененные таким образом требования защиты для различных приложений ИТ рекомендуется зарегистрировать в таблице, которая будет использована в последующей оценке требований защиты систем ИТ. Ниже, в табл. 5, приведен пример заполнения такой таблицы, который показывает главные приложения ИТ, их требования защиты и обоснование (объяснение) после назначения категорий требований защиты.

Таблица 5

Приложение ИТ			Оценка требований защиты		
Номер	Имя	Личные данные	Основной параметр	Требование Защиты	Объяснение
A1	Обработка HR данных	X	Конфиденциальность	Высокая	HR данные составляет особенно чувствительные персональные данные, раскрытие которых может значительно вредить человеку.
			Целостность	Умеренный	Требование защиты только "умеренно", так как ошибки могут быть обнаружены быстро и исправлены.
			Доступность	Умеренный	Время простоя может быть до недели.
A2	Обработка дохода	X	Конфиденциальность	Высокая	Данные дохода включают персональные данные, который имеет особенно высокое требование защиты. Раскрытие этих данных могло быть очень вредно для персонала.

После рассмотрения приложений определяются требования защиты для систем ИТ. Оценка требований защиты для каждой системы ИТ осуществляется на основе рассмотрения всех приложений ИТ, которые имеют прямую ассоциацию с данной системой ИТ. При этом рекомендуется руководствоваться следующими принципами.

Требования защиты конкретной системы ИТ определяются ущербом или суммой наиболее серьезных случаев ущерба соответствующих приложений (**максимальный принцип**)

При изучении возможного ущерба и его значений, необходимо учитывать взаимосвязь приложений ИТ в системе ИТ (одно приложение может использовать результаты других приложений) **(отношения зависимости)**.

В случаях обработки несколько приложений ИТ или наборов информации в одной системе ИТ, необходимо определить возможность проявления совокупного (кумулятивного) эффекта как увеличения ущерба **(совокупный эффект)**, так и уменьшения (**дистрибутивный эффект**).

Результаты оценки требований защиты каждой системы ИТ должны быть задокументированы в табличной форме.

Ниже приведен пример заполнения такой таблицы из Руководства, который показывает системы ИТ, оценки требований защиты для каждой системы в терминах конфиденциальности, целостности и доступности и обоснование (объяснение) после назначения категорий требований защиты (табл.6).

Таблица 6

Система ИТ		Оценка требований защиты		
Номер	Описание	Основной Параметр	Требование	Объяснение
S1	Сервер для Че-	Конфиденциальность	Высокая	Максимальный принцип
		Целостность	Умеренная	Максимальный принцип
		Доступность	Умеренная	Максимальный принцип
S2	Первичный	Конфиденциальность	Умеренная	Максимальный принцип
		Целостность	Высокая	Максимальный принцип

Аналогичным образом проводится оценка требований защиты для линий связи и для помещений, в которых установлены активы ИТ. Оценки проводятся на основе результатов оценки требований защиты ИТ-системи сетевого плана, подготовленного в разделе 2.1 при обследовании активов ИТ. Результаты, полученные на подэтапе «Оценка требований защиты», служат исходными данными для последующих действий по составлению концепции безопасности ИТ.

После завершения подэтапа «Оценка технических требований» следующим этапом создания концепции безопасности ИТ (см. рис.2) является «Анализ базовой защиты ИТ», который включает подэтап «Моделирование базовой защиты ИТ» и подэтап «Проверка базовой безопасности ИТ». Методология проведения данных работ описана соответственно в частях 2.3 и 2.4 главы 2 Руководства.

Моделирование активов ИТ заключается в сравнительном анализе и установлении соответствия каждому компоненту (или группе однотипных компонентов) из плана сети рассматриваемой ИТ определенного унифицированного модуля из Руководства, который содержит набор типовых угроз и защитных мероприятий безопасности. При этом, один и тот же модуль может быть использован несколько раз для сходных организационных компонент активов ИТ.

Для упрощения отображения сложного многообразия активов ИТ на унифицированные модули глав 3 – 9 и исключения дублирования Руководство рекомендует 5-ти уровневую модель, со следующим распределением аспектов безопасности по отдельным уровням.

Уровень 1 «Высший порядок аспектов безопасности ИТ» охватывает все общие аспекты безопасности ИТ, которые универсально применимы к каждому отдельному моделируемому компоненту активов ИТ. Первичными рассматриваемыми элементами являются политики, концепции и полученные из них процедуры. На уровне 1 используются модули 3.1 –3.8 и 9.1.

Уровень 2 «Безопасность инфраструктуры» связан со строительными и структурными условиями функционирования компонентов активов ИТ. Моделируется при помощи унифицированных модулей главы 4 Руководства, применяемых к каждому зданию, помещению, соединению (или группе этих компонентов)

Уровень 3 «Безопасность систем ИТ» рассматривает аспекты безопасности отдельных систем ИТ. И охватывается унифицированными модулями из глав 5, 6, 8 и 9 Руководства, которые применяются как к отдельным системам ИТ так и к выборка из групп.

Уровень 4 «Безопасность в сети» рассматривает аспекты безопасности при организации сети систем ИТ, которые не могут быть изолированы в отдельных системах ИТ и относятся к сетевым подключениям и связи между системами ИТ. Для упрощения рассмотрения Руководство рекомендует разделять большие сети на отдельные законченные подсети в соответствии с двумя критериями:

- оценка требований защиты идентифицировала подключения, по которым некоторые данные ни при каких условиях не должны передаваться. Такие подключения должны рассматриваться как «интерфейсы» между подсетями. И наоборот, подключения, по которым передаются данные, имеющие «высокие» или «очень высокие» требования защиты, не должны пересекать через никакие подсетевые границы;
- компоненты, связанные между собой по удаленному подключению, не должны быть назначены в одну и туже подсеть.

На уровне 4 используются унифицированные модули из глав 6, 7 и 8 Руководства.

Уровень 5 «Безопасность в приложениях» является самым нижним уровнем и рассматривает аспекты безопасности реальных приложений ИТ, которые используются в активах ИТ. Для моделирования должны применяться унифицированные модули из глав 7, 8 и 9 Руководства для каждого приложения.

Модель базовой защиты ИТ, т.е. назначение унифицированных модулей к целевым объектам, должна быть задокументирована в форме таблицы, пример которой приведен в Руководстве представлен ниже в табл. 7

Таблица 7

Номер	Название модуля	Объект-цель / целевая группа	Произведена выборка	Посредник	Примечания
3.1	Организация	Боннский сайт			Модуль Организации должен работать отдельно для Боннских и Берлинских сайтов,.
3.1	Организация	Берлинский сайт			
3.2	Персонал	Полный BOV			Отдел людских ресурсов BOV'S расположен центрально в Бонне.
4.3.3	Архив Носителей данных	R U.02 (Бонн)			резервные средства данных сохраняются в этой комнате
5.3	PC Портативной ЭВМ	C5	1 в R 1.06 (Бонн)		выборка будет выбрана из всех портативных ЭВМ, и в Бонне и Берлине.
5.3	PC Портативной ЭВМ	C6	1 в R 2.01 (Берлин)		
7.5	Сервер WWW	S5			Функции S5 как сервер для Intranet.
9.2	Базы данных	S5			База данных используется на сервере S5.

Результатом моделирования активов ИТ – модель базовой защиты активов ИТ, которая составлена из различных унифицированных модулей глав 3 – 9 Руководства и отражает существенные аспекты безопасности активов ИТ на определенные модули и наоборот. В зависимости от состояния рассматриваемых активов ИТ (находятся в эксплуатации либо планируются) мо-

ель может использоваться в форме тест – плана (в первом случае) либо концептуального про-кта (во - втором случае). В случаях модернизации действующих активов ИТ результирующая модель базовой защиты ИТ будет одновременно и тест – планом и концептуальным проектом, т. к. будет содержать комбинацию уже реализованных защитных мер безопасности и находящихся в стадии планирования.

По завершению моделирования базовой защиты ИТ должна быть выполнена проверка базовой безопасности ИТ. Методология проведения данных работ описана в части 2.4 главы 2 Руководства.

Унифицированный модуль из состава модели базовой защиты ИТ теперь используется как испытательный (тест) план чтобы установить, используя целевое сравнение, путем реального сопоставления, какие стандартные защитные меры безопасности были соответственно осуществлены и какие были не осуществлены либо осуществлены неудовлетворительно. Часть 2.4 главы 2 Руководства описывает, как исполнить проверку базовой безопасности в контексте центральной задачи составления концепции безопасности ИТ и определяет следующие три стадии проведения проверки. Первый стадия - предварительная организация работы и, в частности, выбор соответствующих посредников для целевого сравнения, путем реального сопоставления. На стадии 2 выполняется целевое сравнение, путем реального сопоставления, используя интервью и производя выборочную проверку. На конечной стадии, результаты целевого сравнения, путем реального сопоставления, задокументированы, вместе с обоснованием.

После окончания проверки базовой безопасности должен быть разработан и исполнен план реализации защитных мероприятий безопасности ИТ в соответствии с рекомендациями, изложенными в части 2.6 главы 2 Руководства

Заключение

В заключение данного краткого обзора Руководства по базовой защите ИТ следует отметить следующее.

С позиции пользователей нацеленность Руководства на оказании помощи пользователям в оперативном решении общих задач и упрощении процессов обеспечения безопасности информационных технологий безусловно является положительным фактором.

Вместе с тем, поскольку информационные технологии постоянно развиваются, BSI каждые шесть месяцев модифицирует и расширяет Руководство путем переделки (модификации) существующих либо добавлением новых компонент (структурных модулей, процедур, угроз и т. д.). Таким образом, границы понятий «разумный и достаточный уровень защиты ИТ» и «уровень базовой защиты ИТ» зыбкие и неопределенные. Аналогично обстоит дело и с понятиями «совокупность идентифицированных мероприятий безопасности» и «типичные» системы ИТ. Кроме того, в случае наличия ИТ-системс высокими либо очень высокими требованиями защиты Руководство в части 2.5 главы 2 методологически дополнительный анализ безопасности возлагает на пользователей. Сформированные пользователями по результатам анализа защитные меры безопасности будут отсутствовать в текущей редакции Руководства, и, при определенных условиях, будут включены BSI в последующие редакции. Вследствие этого, при сравнении двух редакций возникает вопрос что понимать под «уровнем базовой защиты ИТ».

Данные обстоятельства, на наш взгляд, не позволяют в принципе ввести четкую иерархию классов защищенности (безопасности) ИТ, в отличие от таких нормативных документов, как международный стандарт ISO 15408 и отечественные НД ТЗИ 2.5-004-99 Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа и НД ТЗИ 2.5-005 –99 Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа. По этой причине возможность применение данного документа в целях сертификации ИТ проблема-

тична, хотя эти вопросы находится в состоянии обсуждения.

По мнению авторов, Руководство целесообразно применять в дополнение указанным стандартам в целях облегчения процессов определения перечня угроз и совокупности защитных мер безопасности ИТ.

Список литературы 1 *И. Д. Горбенко, д-р техн. наук, А. В. Потий, канд. техн. наук,П. И. Терещенко.* Критерии и методология оценки безопасности информационных технологий// Радиотехника. Всеукр. межвед. науч.-техн сб. 2000. Вып. 114, С 25-38. 2. *ISO/IEC 15408* Information technology - Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements. 3. *German Information Security Agency.* IT Baseline Protection Manual - Standard security safeguards. *2000.*

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11.04.2002.