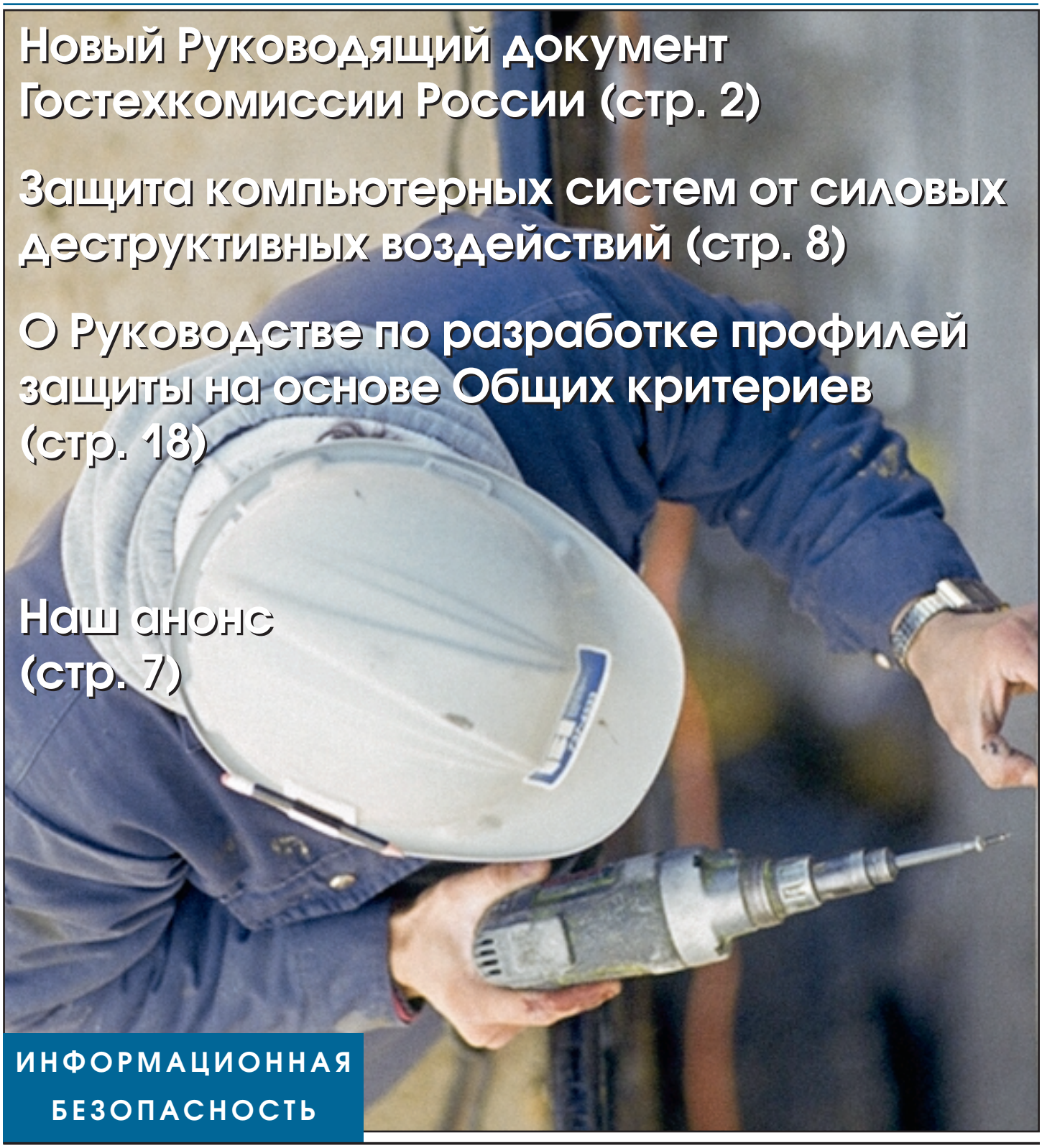
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 2 (81)/2000



Новый Руководящий документ Гостехкомиссии России (стр. 2)

Защита компьютерных систем от силовых деструктивных воздействий (стр. 8)

О Руководстве по разработке профилей защиты на основе Общих критериев (стр. 18)

Наш анонс (стр. 7)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ГОСТЕХКОМИССИЯ РОССИИ

РУКОВОДЯЩИЙ ДОКУМЕНТ

Защита от несанкционированного доступа к информации

Часть 1.

Программное обеспечение средств защиты информации

Классификация по уровню контроля отсутствия недекларированных возможностей

Введен в действие Приказом Председателя Гостехкомиссии России №114 от 4.06.99 г.

1999

Настоящий Руководящий документ (РД) устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Действие документа не распространяется на программное обеспечение средств криптографической защиты информации.

Уровень контроля определяется выполнением заданного настоящим РД набора требований, предъявляемого:

- к составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ;
- к содержанию испытаний.

Руководящий документ разработан в дополнение РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», М., Военное издательство, 1992 г., РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», М., Военное издательство, 1992 г. и РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», М., 1997 г.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия недекларированных возможностей.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. *Классификация* распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1.2. Устанавливается *четыре уровня контроля* отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований.

1.3. Для ПО, используемого при защите информации, **отнесенной к государственной тайне**, должен быть обеспечен уровень контроля не ниже **третьего**.

1.4. Самый высокий уровень контроля — ***первый***, достаточен для ПО, используемого при защите информации с грифом «ОВ».

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».

1.5 Самый низкий уровень контроля — ***четвертый***, достаточен для ПО, используемого при защите **конфиденциальной** информации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. *Недекларированные возможности* — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Реализацией недекларированных возможностей, в частности, являются программные закладки.

2.2. *Программные закладки* — преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

2.3. *Функциональный объект* — элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы.

В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п.

2.4. *Информационный объект* — элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т.п.

2.5. *Маршрут выполнения функциональных объектов* — определенная алгоритмом последовательность выполняемых функциональных объектов.

2.6. *Фактический маршрут выполнения функциональных объектов* — последовательность фактически выполняемых функциональных объектов при определённых условиях (входных данных).

2.7. *Критический маршрут выполнения функциональных объектов* — такой маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов.

2.8. *Статический анализ исходных текстов программ* — совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ.

2.9. *Динамический анализ исходных текстов программ* — совокупность методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа.

3. ТРЕБОВАНИЯ К УРОВНЮ КОНТРОЛЯ

3.1. Перечень требований

См. табл. 1.

3.2. Требования к четвертому уровню контроля

3.2.1. Контроль состава и содержания документации

В состав документации, представляемой заявителем, должны входить:

№	Наименование требования	Уровень контроля			
		4	3	2	1
	Требования к документации				
1	**Контроль состава и содержания документации**				
1.1.	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2.	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3.	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4.	Пояснительная записка (ГОСТ 19.404-79)	–	+	=	=
1.5.	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2.	**Контроль исходного состояния ПО**	+	=	=	=
3.	**Статический анализ исходных текстов программ**				
3.1.	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2.	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3.	Контроль связей функциональных объектов по управлению	–	+	=	=
3.4.	Контроль связей функциональных объектов по информации	–	+	=	=
3.5.	Контроль информационных объектов	–	+	=	=
3.6.	Контроль наличия заданных конструкций в исходных текстах	–	–	+	+
3.7.	Формирование перечня маршрутов выполнения функциональных объектов	–	+	+	=
3.8.	Анализ критических маршрутов выполнения функциональных объектов	–	–	+	=
3.9.	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т.п., построенных по исходным текстам контролируемого ПО	–	–	+	=
4.	**Динамический анализ исходных текстов программ**				
4.1.	Контроль выполнения функциональных объектов	–	+	+	=
4.2.	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	–	+	+	=
5.	**Отчетность**	+	+	+	+

Табл. 1. Перечень требований.

Обозначения: «–» — нет требований к данному уровню; «+» — новые или дополнительные требования; «=» — требования совпадают с требованиями предыдущего уровня.

- спецификация (**ГОСТ 19.202-78**), содержащая сведения о составе ПО и документации на него;
- описание программы (**ГОСТ 19.402-78**), содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;
- описание применения (**ГОСТ 19.502-78**), содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы;
- исходные тексты программ (**ГОСТ 19.401-78**), входящих в состав ПО.

Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям указанных ГОСТ.

3.2.2. Контроль исходного состояния ПО

Контроль заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации.

Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО.

Контрольные суммы должны рассчитываться для *каждого файла*, входящего в состав ПО.

3.2.3. Статический анализ исходных текстов программ

Статический анализ исходных текстов программ должен включать следующие технологические операции:

- контроль полноты и отсутствия избыточности исходных текстов ПО *на уровне файлов*;
- контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.

3.2.4. Отчетность

По окончании испытаний оформляется отчет (протокол), содержащий результаты:

- контроля исходного состояния ПО;
- контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;
- контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.

3.3. Требования к третьему уровню контроля

3.3.1. Контроль состава и содержания документации

Требования полностью включают в себя аналогичные требования к четвертому уровню контроля.

Кроме того, должна быть представлена «**Пояснительная записка**» (**ГОСТ 19.404-79**), содержащая основные сведения о назначении компонентов, входящих в состав ПО, параметрах обрабатываемых наборов данных (подсхемах баз данных), формируемых кодах возврата, описание используемых переменных, алгоритмов функционирования и т.п.

3.3.2. Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования к четвёртому уровню контроля.

3.3.3. Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к четвёртому уровню контроля, дополнительно предъявляются следующие требования:

- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне *функциональных объектов (процедур)*;
- контроль связей функциональных объектов (*модулей, процедур, функций*) по управлению;
- контроль связей функциональных объектов (*модулей, процедур, функций*) по информации;
- контроль информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);
- формирование перечня маршрутов выполнения функциональных объектов (*процедур, функций*).

3.3.4. Динамический анализ исходных текстов программ

Динамический анализ исходных текстов программ должен включать следующие технологические операции:

- контроль выполнения функциональных объектов (*процедур, функций*);
- сопоставление фактических маршрутов выполнения функциональных объектов (*процедур, функций*) и маршрутов, построенных в процессе проведения статического анализа.

3.3.5. Отчетность

Кроме аналогичных требований, предъявляемых к четвертому уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

- контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на *уровне функциональных объектов (процедур)*;
- контроля связей функциональных объектов (модулей, процедур, функций) по управлению;
- контроля связей функциональных объектов (модулей, процедур, функций) по информации;
- контроля информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.);
- формирования перечня маршрутов выполнения функциональных объектов (процедур, функций);
- контроля выполнения функциональных объектов (*процедур, функций*);
- сопоставления фактических маршрутов выполнения функциональных объектов (*процедур, функций*) и маршрутов, построенных в процессе проведения статического анализа.

3.4. Требования ко второму уровню контроля

3.4.1. Контроль состава и содержания документации

Требования полностью включают в себя аналогичные требования к третьему уровню контроля.

3.4.2. Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования к третьему уровню контроля.

3.4.3. Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:

- контроль полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне *функциональных объектов (функций)*;
- *синтаксический* контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных программных конструкций;
- формирование перечня маршрутов выполнения *функциональных объектов (ветвей)*;
- анализ критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков *информационных объектов*;
- построение по исходным текстам контролируемого ПО блок-схем, диаграмм и т.п., и последующий сравнительный анализ алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведенного в «Пояснительной записке».

3.4.4. Динамический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно предъявляются следующие требования:

- контроль выполнения функциональных объектов (*ветвей*);
- сопоставление фактических маршрутов выполнения функциональных объектов (*ветвей*) и маршрутов, построенных в процессе проведения статического анализа.

3.4.5. Отчетность

Кроме аналогичных требований, предъявляемых к третьему уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

- контроля полноты и отсутствия избыточности исходных текстов контролируемого программного обеспечения на уровне функциональных объектов (функций);
- *синтаксического* контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций;
- формирования перечня маршрутов выполнения функциональных объектов (ветвей);
- анализа критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков информационных объектов;
- построения по исходным текстам контролируемого ПО блок-схем, диаграмм и т.п., и последующего сравнительного анализа алгоритма работы функциональных объектов (*процедур, функций*) и алгоритма работы, приведённого в «*Пояснительной записке*»;
- контроля выполнения функциональных объектов (*ветвей*);
- сопоставления фактических маршрутов выполнения функциональных объектов (ветвей) и маршрутов, построенных в процессе проведения статического анализа.

3.5. Требования к первому уровню контроля

3.5.1. Контроль состава и содержания документации

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.2. Контроль исходного состояния ПО

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.3. Статический анализ исходных текстов программ

Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно предъявляются следующие требования:

- контроль соответствия исходных текстов ПО его объектному (загрузочному) коду *с использованием сертифицированных компиляторов*;
- *семантический* контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций.

3.5.4. Динамический анализ исходных текстов программ

Требования полностью включают в себя аналогичные требования ко второму уровню контроля.

3.5.5. Отчетность

Кроме аналогичных требований, предъявляемых ко второму уровню контроля, дополнительно отчет (протокол) должен содержать результаты:

- контроля соответствия исходных текстов ПО его объектному (загрузочному) коду *с использованием сертифицированных компиляторов*;
- семантического контроля наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных конструкций.

Наш анонс

Опубликована справочная информация Гостехкомиссии России

Наряду с «регулярной» частью номера 2 за 2000 год, в виде специального выпуска публикуется приложение, содержащее справочную информацию Государственной Технической Комиссии при Президенте Российской Федерации. В приложение вошли следующие перечни:

- перечень предприятий и организаций, получивших лицензии на деятельность в области защиты информации;
- государственный реестр сертифицированных средств защиты информации;
- перечень сертифицированных средств защиты информации, на которые срок действия сертификатов истек (в Jet Info публикуется впервые);
- перечень лицензионных центров в области защиты информации;
- перечень органов по сертификации Системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России;
- перечень испытательных лабораторий Системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России;
- перечень органов по аттестации Системы сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России.

Справочная информация представлена по состоянию на 29 февраля 2000 года.

Как показывает статистика обращений к серверу Jet Info Online, материалы Гостехкомиссии России неизменно привлекают внимание. Особенно популярны перечень лицензиатов и реестр сертифицированных средств защиты информации.

На сервере Jet Info Online справочная информация Гостехкомиссии России и ФАПСИ РФ регулярно обновляется. Теперь подобное обновление затронуло и «бумажный» вариант бюллетеня. Мы надеемся, что новый специальный выпуск Jet Info поможет руководителям и техническим специалистам в их работе по обеспечению информационной безопасности.

Защита компьютерных систем от силовых деструктивных воздействий

Вячеслав Барсуков,
кандидат технических наук

СОДЕРЖАНИЕ

1. Введение

Данная статья посвящена методам защиты от **Силового Деструктивного Воздействия (СДВ)** – резкого всплеска напряжения в сетях питания, коммуникаций или сигнализаций с амплитудой, длительностью и энергией всплеска, способными привести к сбоям в работе оборудования или к его полной деградации. Знание этих методов позволяет повысить безопасность компьютерных систем или, в более широком плане, систем с компьютерными компонентами.

Технические средства силового деструктивного воздействия (ТС СДВ) являются, по существу, **электромагнитным оружием**, которое способно дистанционно и без лишнего шума поразить практически любую компьютерную систему. Главное – обеспечить соответствующую мощность электромагнитного импульса. Существенно повышает скрытность нападения то обстоятельство, что анализ повреждений в уничтоженном оборудовании не позволяет однозначно идентифицировать причину возникновения повреждения, так как причиной может быть как преднамеренное (нападение), так и непреднамеренное (например, индукция от молнии) силовое деструктивное воздействие. Это, к сожалению, упрощает многократное успешное использование ТС СДВ.

2. Каналы силового деструктивного воздействия на компьютерные системы

Проведенный анализ показывает, что компьютер или любое другое электронное оборудование могут быть подвергнуты силовому деструктивному воздействию по трем основным **каналам (КСДВ)**:

- **по сети питания** (КСДВ-1);
- **по проводным линиям** (КСДВ-2);
- **по эфиру** с использованием мощных коротких электромагнитных импульсов (КСДВ-3).

В качестве примера на рис. 1 показаны основные каналы деструктивного воздействия на компьютер, являющийся ядром интегрированной системы безопасности.

Для проникновения энергии СДВ по сети питания имеется два основных канала:

- кондуктивный путь через вторичный источник питания (ВИП);
- наводки через паразитные емкостные и индуктивные связи, как внутренние, так и внешние (например, через сигнальные цепи и линии связи).

В качестве примера проведем оценку устойчивости компонентов основного элемента питания компьютерной системы — вторичного источника питания, типовая принципиальная схема которого приведена на рис.2.

Результаты оценки устойчивости элементов типового блока вторичного источника питания приведены в табл. 1.

Как видно из табл.1, элементы входного LC-фильтра имеют весьма низкую энергопоглощающую способность и не являются защитой против мощных импульсных помех. Поэтому, если LC-фильтр — единственное устройство защиты на входе ВИП, то нападающему для достижения цели достаточно обеспечить возможность подвода мощной импульсной помехи с амплитудой 2 кВ, энергией 1...2 Дж и длительностью импульса не менее 1с (зона СДВ 1 рис.1).

В современных ВИП основные функции защиты от мощных помех принимает на себя варистор. Однако, несмотря на большие уровни рабочих токов, они имеют предельно допустимую рассеиваемую мощность в единицы ватт, поэтому при воздействии длинных импульсов с относительно небольшим током они выходят из строя, вызывая сгорание предохранителя на входе. В этом случае в ТС СДВ необходима энергия 50...100 Дж, амплитуда — 1 кВ, длительность импульса — 0,1 с (зона СДВ 2 рис.1).

Для вывода из строя конденсаторов входного фильтра инвертора и диодов моста в ТС СДВ требуется значительно меньшая энергия, причем, чтобы обойти варисторную защиту, используют разницу в напряжении пробоя конденсаторов и напряжения эффективного ограничения напряжения варистором, которая составляет 70...120 В. Задача силового воздействия решается путем использования импульсов длительностью до 5 мс, амплитудой 500...600 В и энергией 15...25 Дж (зона СДВ 3 рис.1). В этом случае после пробоя конденсаторов дополнительно возникает импульс тока через диоды моста, который для горячего термистора доходит до 1000 А, что выводит диоды из строя. При таком воз-

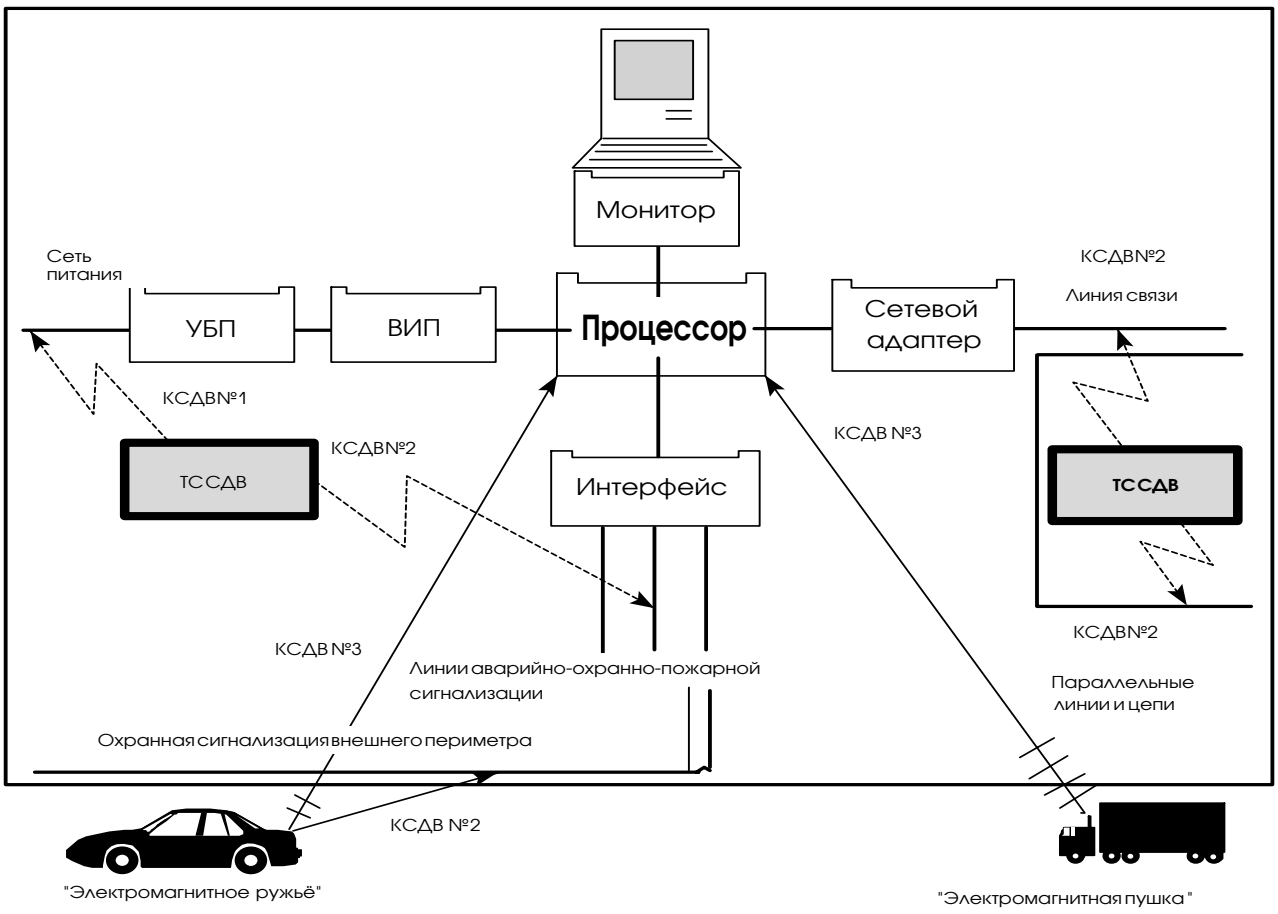


Рис. 1. Основные каналы силового деструктивного воздействия на интегрированную систему безопасности

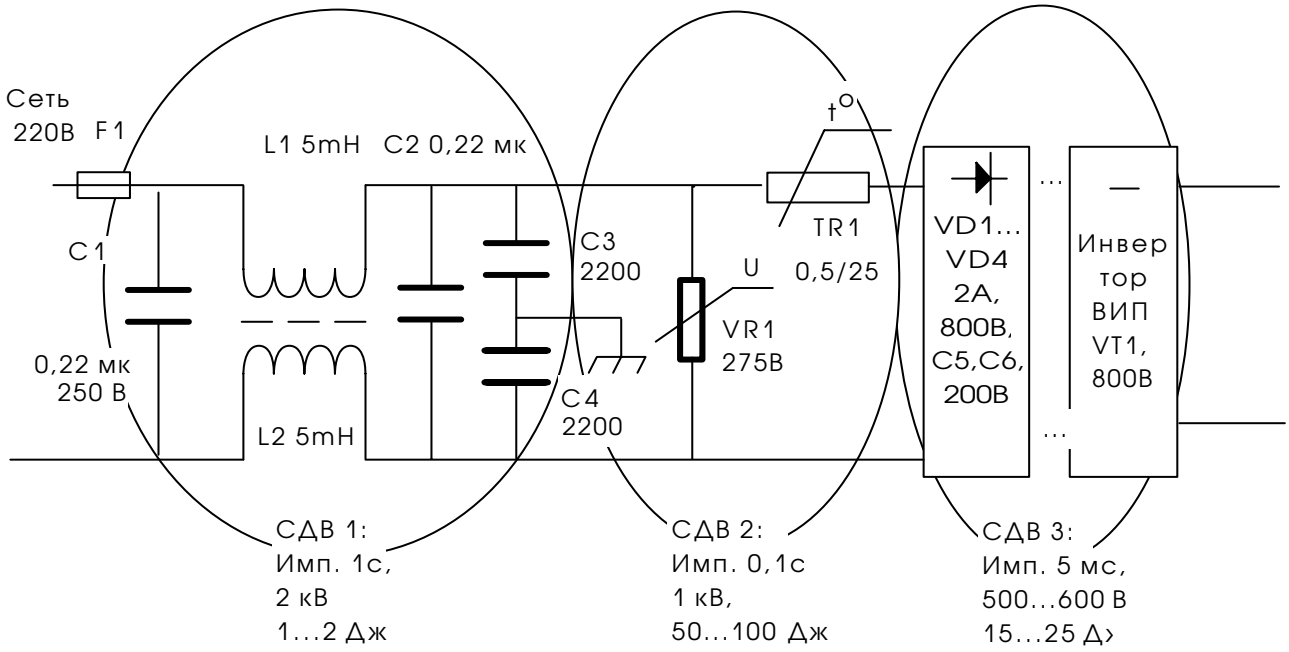


Рис. 2. Принципиальная схема типового блока вторичного источника питания.

действии весьма вероятен выход из строя транзисторов и других элементов инвертора, а также проход деструктивных импульсов на выход ВИП, что приведет к повреждению других узлов компьютерной системы.

Особо необходимо отметить возможность мощного силового деструктивного воздействия с использованием наводок через паразитные емкости между элементами и узлами схемы. Установлено, что входные высоковольтные и выходные низковольтные цепи ВИП компьютеров (например, ПК) имеют емкостную связь через паразитную емкость, равную 10...30 пФ, а паразитная емкость, равная 5...10 пФ, связывает сеть питания с элементами материнской платы. Через эти паразитные емкости имеется возможность путем генерации в ТС СДВ высоковольтных импульсов с наносекундным временем нарастания полностью блокировать работу программно-аппаратных средств, в том числе обеспечить искажение данных, зависание компьютеров и сбои в работе программного обеспечения. Эти возможности деструктивного воздействия предъявляют дополнительные требования к защите от импульсных помех.

Как видно из рис. 1, между сетью питания и ВИП, как правило, устанавливается устройство бесперебойного питания (УБП), которое необходимо учитывать при оценке устойчивости к СДВ. УБП предназначены для улучшения качества энергии сети переменного тока и обеспечения бесперебойного электропитания оборудования при выходе из строя электросети. Как правило, в состав УБП входят следующие функциональные узлы:

- входной фильтр-ограничитель перенапряжений;
- зарядное устройство для аккумуляторов;
- аккумуляторный блок;
- преобразователь напряжения или инвертор;
- переключатель каналов;
- стабилизирующий каскад;
- система управления.

По способу управления УБП разделяются на offline и online типы. Главное различие заключается в выборе основного канала передачи энергии к потребителю.

Для типа offline в основном режиме переключатель каналов подключает вход УБП к выходу через ветвь, содержащую только входной фильтр. При этом аккумуляторы подзаряжаются от маломощного зарядного устройства, а напряжение с инвертора не поступает на выход источника. В режиме аккумуляторной поддержки, когда входное напряжение отклоняется от допустимых пределов или пропадает, переключатель каналов подключает ветвь, содержащую инвертор, и энергия к потребителю поступает от аккумуляторов.

Тип online характеризуется постоянством включения ветви, содержащей мощное зарядное устройство, аккумулятор и инвертор на выход блока УБП. Подобная схема позволяет не только исключить время переключения, но и обеспечить гальваническую развязку вход-выход, иметь стабильное синусоидальное выходное напряжение. При выходе из строя какого-либо каскада в прямой ветви передачи энергии, перегрузках, а также при разряде аккумуляторов, переключатель каналов подключает ветвь, соединяющую вход-выход через фильтр. Этот вспомогательный путь передачи энергии, получивший название байпас, имеет особое значение при СДВ и позволяет обойти защиту УБП для поражения более важных блоков компьютерной системы.

Обозначение элемента	Тип элемента	Энергопоглощающая способность, Дж	Предельная поглощающая способность, Дж	Прочность изоляции, В	Примечание
C1, C2	Конденсатор	0,3		1200	Рабочее напряжение: 250 В – переменное, 1000 В – постоян.
L1, L2	Дроссель	0,1		2500	Главное – изоляция между катушками
C3, C4	Конденсатор	0,002		1200	
VR1	Варистор	20/ 40/ 70/ 140 соотв. для диаметра 7/10/14/20 мм	(3...4000) x 10^{-3}		Быстродействие 25 нс, от наносекундных помех оборудование не защищает
VD1...VD4	Полупроводниковый диод	менее 1	(0,1...1000) x 10^{-3}	600...1000	Допустимая амплитуда импульса тока 60/100/200 А для микросборок на 2/3/4 А
VT1	Транзистор	менее 1	(20...1000) x 10^{-3}	500...800	
C5, C6	Конденсатор	15		500	Изоляция может быть пробита при длительности импульса не менее 0,5 мс

Табл. 1. Результаты оценки устойчивости элементов ВИП к воздействию СДВ

Помимо рассмотренных выше типов, в последнее время появились линейно-интерактивные УБП, которые являются дальнейшим развитием технологии offline. Они отличаются наличием на входе стабилизирующего автотрансформатора, что способствует стабилизации выходного напряжения УБП. В некоторых случаях, если допустимы перерывы в питании на несколько миллисекунд, линейно-интерактивные УБП оказываются предпочтительнее типа offline и дешевле online устройств.

Анализируя слабые стороны УБП, нельзя забывать и о заложенных в них возможностях защиты от:

- выходных и внутренних коротких замыканий;
- входной и выходной перегрузки;
- глубокой разрядки аккумуляторов;
- превышения максимальной температуры.

Обычно при СДВ по сети питания УБП выходит из строя, причем в этом случае срабатывает байпас и через него энергия ТС СДВ достигает цели в обход УБП. Кроме того, как правило, у тиристорных стабилизаторов, корректоров напряжения, переключателей сети при СДВ происходит самопроизвольное отпирание тиристоров вопреки штатному алгоритму схемы управления с аварийным отключением или выходом из строя.

Таким образом, **традиционные устройства защиты питания не только не защищают компьютерные системы от СДВ, но и сами подвержены деструктивному воздействию**.

Для проникновения энергии СДВ **по проводным линиям** необходимо преодолеть предельную поглощающую способность компонентов, которые могут быть использованы во входных цепях. Анализ показывает, что для деградации этих компонентов (микросхем, транзисторов, диодов и т.п.) достаточно воздействия импульса с энергией 1 — 1000 мкДж, причем этот импульс может быть весьма коротким, так как время пробоя МОП-структуры или pn-перехода составляет 10—1000 нс. Как известно, напряжения пробоя переходов составляют от единиц до десятков вольт. Так у арсенидгаллиевых приборов это напряжение равно 10 В, запоминающие устройства имеют пороговые напряжения около 7 В, логические ИС на МОП-структурах — от 7 до 15 В. И даже кремниевые сильноточные биполярные транзисторы, обладающие повышенной прочностью к перегрузкам, имеют напряжение пробоя в диапазоне от 15 до 65 В. Отсюда можно сделать вывод, что **для СДВ по проводным каналам требуется энергия на несколько порядков ниже, чем по сети питания** и деструктивное воздействие может быть реализовано с помощью относительно простых технических средств, обеспечивающих высокую вероятность вывода объекта атаки из строя.

При определении уровня защиты от СДВ необходимо учитывать наличие на входе устройств защиты от импульсных помех. В этом случае защищенные компоненты имеют существенно большую предельную энергопоглощающую способность (до 1-10 Дж для низкоскоростных устройств и до 1-10 мДж — для высокоскоростных). Однако из-за высоких цен качественные устройства защиты пока не получили в России широкого применения.

Наиболее скрытым и эффективным является канал силового деструктивного воздействия **по эфиру с использованием мощного короткого электромагнитного импульса**. Можно реализовать компактные электромагнитные технические средства СДВ, размещаемые за пределами объекта атаки на достаточном для маскировки атаки удалении. Конструкция электромагнитного ТС СДВ на примере генератора с виртуальным катодом (виркатора) приведена на рис.3.

Как видно из рисунка, конструкция виркатора является весьма простой. Столь же просто можно описать принцип его работы. При подаче на анод положительного потенциала порядка $10^5 - 10^6$ В вследствие взрывной эмиссии с катода к аноду устремляется поток электронов, который, пройдя через сетку анода, начинает тормозиться собственным «кулоновским полем». Это поле отражает поток электронов обратно к аноду, образуя виртуальный катод. Пройдя через анод в обратном направлении, поток электронов вновь тормозится у поверхности реального катода. В результате такого взаимодействия формируется облако электронов, колеблющееся между виртуальным и реальным катодами. Образованное на частоте колебаний электронного облака СВЧ-поле излучается антенной через обтекатель в пространство. Токи в виркаторах, при которых возникает генерация, составляют величины 1-10 кА. Экспериментально от виркаторов уже получены мощности от 170 кВт до 40 ГВт в сантиметровом и дециметровом диапазонах.

Инжекция мощного электромагнитного импульса у такого ТС СДВ производится с помощью специальной антенной системы, от эффективности которой во многом зависят оперативно-технические характеристики всего комплекса СДВ. Несмотря на наличие направленной антенны, мощный электромагнитный импульс воздействует при атаке объекта на все компоненты в пределах зоны электромагнитного воздействия и на все контуры, образованные связями между элементами оборудования, поэтому, не являясь еще средствами селективного воздействия, ТС СДВ наносят глобальные поражения, оправдывая установившееся название «электромагнитной бомбы».

Актуальность проблемы защиты от электромагнитного СДВ возрастает еще и потому, что в настоящее время некоторые исследовательские работы закончились созданием опытных образцов информационного оружия. Так, вызывает интерес американский образец оружия данного класса под условным названием MPS-II, который представляет собой генератор высокомощного СВЧ-излучения, использующий зеркальную антенну диаметром 3 м. Данный образец развивает импульсную мощность

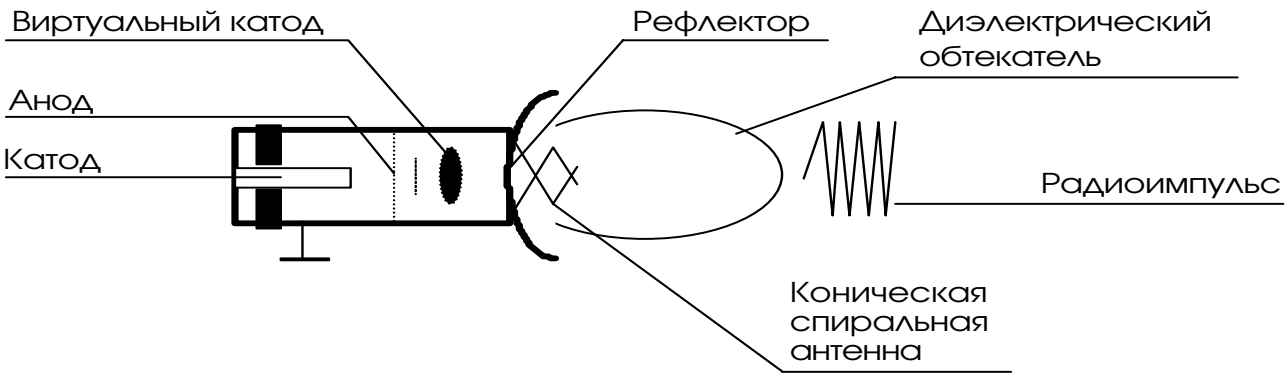


Рис.3. Конструкция высокочастотного электромагнитного ТС СДВ.

Рис. 4. Классификация технических средств СДВ по сетям питания.

Рис. 5. Классификация ТС СДВ по проводным линиям.

около 1 ГВт (напряжение 265 кВ, ток 3,5 кА) и обладает большими возможностями ведения информационной войны. В руководстве по применению и техническому обслуживанию определена основная его характеристика: зона поражения — 800 м от устройства в секторе 24 градуса [1]. Используя подобную установку, можно эффективно выводить из строя компьютерную технику, стирать записи на магнитных носителях, в кредитных карточках и т.п.

Использование новых технологий, в частности, фазированных антенных решеток, позволяет осуществить СДВ сразу на несколько целей. Примером может служить система GEM2, разработанная по заказу фирмы Boeing южно-африканской фирмой PCI. Эта система состоит из 144 твердотельных излучателей импульсов длительностью менее 1 нс с суммарной мощностью 1 ГВт и может устанавливаться на подвижных объектах.

Приведенные данные говорят о больших возможностях и высокой эффективности нового информационного оружия, что необходимо учитывать при обеспечении защиты информации, тем более, что во время войны в Персидском заливе уже было зафиксировано боевое применение подобного оружия в ракетном варианте [2]. Конечно рассмотренные примеры относятся к военным технологиям, однако история и реальная действительность, к сожалению, показывают, что интервалы времени между разработкой военной технологии и возможностью её широкого использования год от года становяться все меньше и меньше.

3. Классификация средств силового деструктивного воздействия

3.1. Технические средства СДВ по сетям питания

В предыдущем разделе было установлено, что для вывода из строя элементной базы компьютерных систем, систем сигнализации и охраны может быть использовано силовое деструктивное воздействие **по сетям питания**. Для осуществления СДВ используются специальные технические средства, которые подключаются к сети непосредственно с помощью гальванической связи через конденсатор или с помощью индуктивной связи через трансформатор. Прогнозы специалистов показывают, что **вероятность использования СДВ растет год от года**. Поэтому при разработке концепции безопасности объекта необходимо учитывать и возможность СДВ по сетям питания, для чего, в первую очередь, необходимо провести классификацию технических средств СДВ. Однако, учитывая специфическое назначение данных средств и нежелание фирм, их производящих, афишировать свою деятельность, задача классификации оказалась нетривиальной. Возможная классификация современных технических средств СДВ по сетям питания, проведенная по результатам анализа, представлена на рис.4.

Представленная на рис. 4 классификация пояснений не требует, за исключением класса «Специальные и другие ТС СДВ». К этому классу отнесены, в частности, различные суррогатные ТС СДВ, имеющиеся под рукой. Например, в качестве технического средства воздействия может быть использована ближайшая трансформаторная подстанция, к части вторичной обмотки которой можно подключить ТС СДВ с емкостным накопителем, параметры которого подобраны так, что вторичная обмотка трансформатора, магнитопровод и емкостной накопитель образуют повышающий резонансный автотрансформатор. Такое силовое воздействие может вывести из строя все электронное оборудование, обслуживаемое данной подстанцией. К этому же классу отнесены и средства перепрограммирования ИБП с использованием, например, программных закладок. Такая закладка может быть активизирована соответствующей командой по сети электропитания, чтобы на короткое время перепрограммировать ИБП на максимально возможное выходное напряжение, что также приведет к выходу из строя подключенного к нему электронного оборудования.

В качестве примера высокой эффективности деструктивного воздействия ТС СДВ можно отметить относительно недорогие устройства с электро-

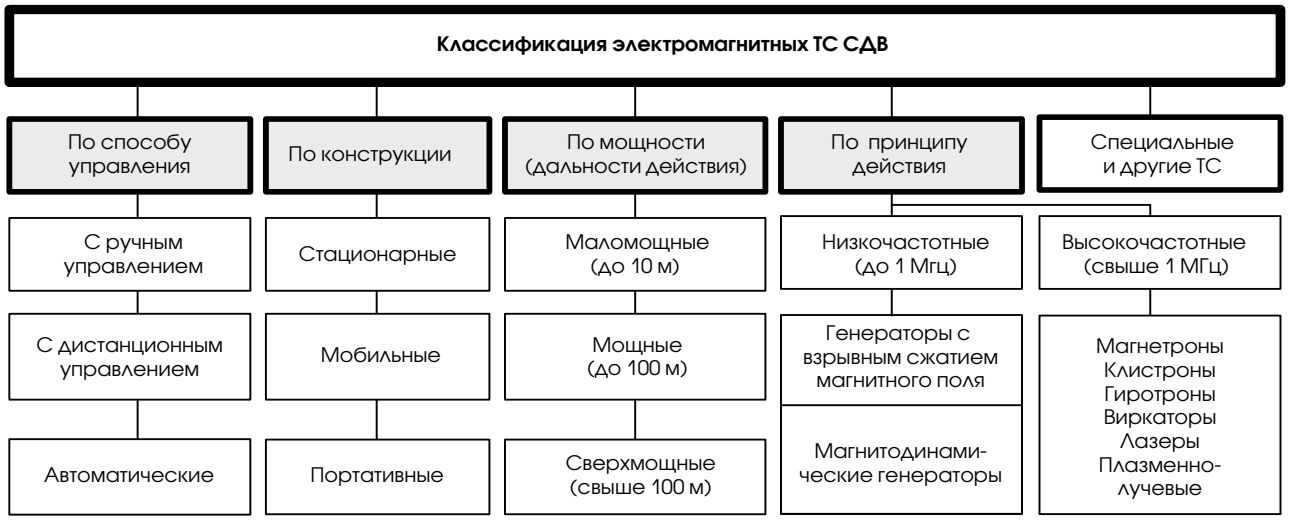


Рис.6. Классификация ТС СДВ по эфиру (электромагнитных ТС СДВ).

литическими конденсаторами, имеющие удельную объемную энергию, равную 2000 кДж/м^3. Подобное устройство, размещенное в обычном кейсе, способно вывести из строя до 20 компьютеров одновременно. Ориентировочная стоимость такого кейса составляет от 10000 до 15000 долларов США. Ещё большую эффективность имеют молекулярные накопители (ионисторы), удельная объемная энергия которых достигает 10 МДж/м^3. ТС СДВ, содержащее ионисторы, уже способно вывести из строя все компьютеры большого вычислительного центра. Стоимость такого технического средства ориентировочно составляет 50000 долларов США (стоимость и энергетические параметры ТС СДВ приведены для оценки эффективности защиты).

3.2. Технические средства СДВ по проводным каналам

Для деструктивного воздействия на системы безопасности по **проводным линиям** требуется существенно меньшая энергия и длительность импульсов, чем для СДВ по сетям питания. Поэтому ТС СДВ по проводным каналам имеют более простую схемотехнику и возможность использования автономных источников питания и, как следствие, существенно меньшие габариты и цену, чем их сетевые аналоги. Так, например, ТС СДВ с низковольтным емкостным накопителем большой энергии может быть реализовано в размерах среднего кейса при стоимости от 6000 до 8000 долларов. В то же время, необслуживаемое ТС СДВ с емкостной развязкой имеет размеры видеокассеты и стоит порядка 1000-1500 долларов. Классификация ТС СДВ по проводным каналам приведена на рис. 5.

Как видно из рис.5, в данной классификации все нетрадиционные и специфические ТС СДВ отнесены к классу «Специальные и другие технические средства». Так, например, в составе некоторых средств деструктивного воздействия в качестве инжекторов могут быть использованы конструкционные элементы здания, канализация, водопровод, сеть питания объекта и т.п.

3.3. Технические средства СДВ по эфиру

Анализ показывает, что наиболее опасными ТС СДВ являются **технические средства силового деструктивного воздействия по эфиру** с использованием электромагнитного импульса (электромагнитные ТС СДВ). В наибольшей степени это относится к мощным мобильным ТС СДВ, деструктивное действие которых может осуществляться с неохраняемой территории. К сожалению, недостаток открытой информации по данному виду ТС СДВ существенно осложняет их классификацию. Классификация электромагнитных ТС СДВ, использованная в данной работе, приведена на рис. 6.

Проводя анализ возможностей использования ТС СДВ, необходимо отметить, что наиболее удобными в применении и наиболее продвинутыми в исследованиях являются высокочастотные электромагнитные средства СДВ, в том числе магнетроны, клистроны, гиротроны, лазеры на свободных электронах, плазменно-лучевые генераторы, а также рассмотренные выше виркаторы, которые, хотя и имеют низкий КПД (единицы процентов), но легче всего перестраиваются по частоте. Наиболее широкополосными являются плазменно-лучевые генераторы, а особенностью гиротронов является то, что они работают в миллиметровом диапазоне с высоким КПД (десятки процентов).

Исторически одним из первых образцов электромагнитного оружия, которое было продемонстрировано еще в конце 50-х годов в лос-аламосской национальной лаборатории США, является генератор с взрывным сжатием магнитного поля [2]. В дальнейшем в США и СССР было разработано и испытано множество модификаций такого генератора, развивавших энергию воздействия в десят-

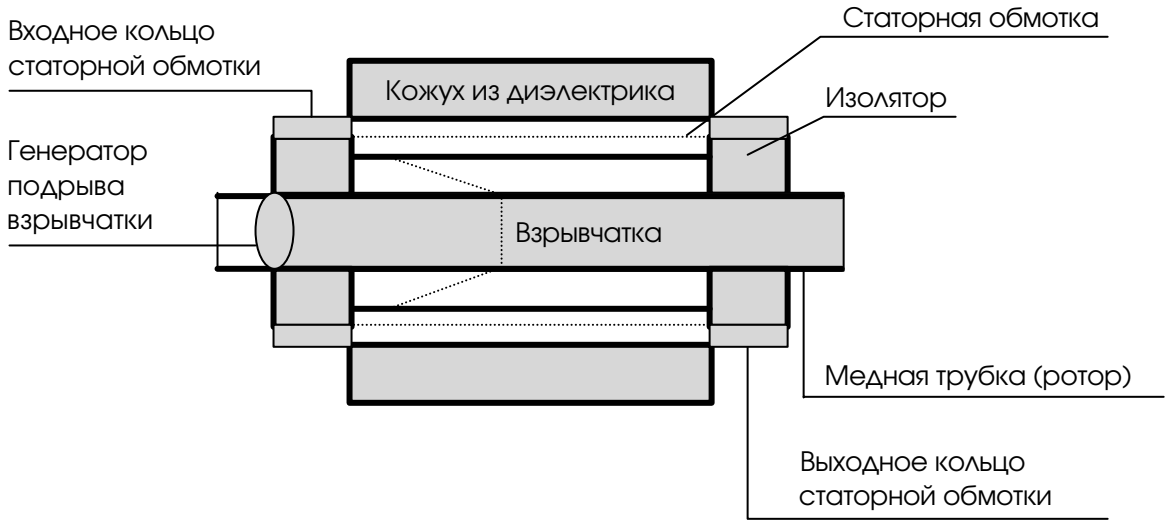


Рис.7. Схема генератора с взрывным сжатием магнитного поля.

№ п/п	Рекомендация по защите компьютерных систем от СДВ	Примечание
	Общие организационно-технические мероприятия	
1.	Провести анализ схем электроснабжения, внутренних и внешних коммуникационных каналов объекта, а также линий аварийно-охранно-пожарной сигнализации для выявления возможных путей СДВ	К анализу привлекаются квалифицированные специалисты-электрики и связисты
2.	Произвести разделение объекта на зоны защиты и рубежи обороны: • 1-й рубеж- защита по периметру объекта; • 2-й рубеж- защита поэтажная; • 3-й рубеж-индивидуальная защита	Для небольших объектов (офисов) 1-й рубеж может отсутствовать, а 2-й рубеж сокращается до защиты отдельного помещения
3.	После проведения монтажа компьютерных систем провести тестирование на реальные воздействия	Для тестирования используются специальные имитаторы СДВ
4.	Разработать документы ограничительного характера, направленные на уменьшение возможности использования ТС СДВ	Например, запретить использование розеток выделенной сети для пылесосов и другого оборудования, в которые могут быть встроены ТС СДВ
5.	Ремонтные работы и текущее обслуживание электрооборудования, линий связи и цепей сигнализации компьютерной системы необходимо производить под контролем службы безопасности	Необходимо фиксировать все проведенные доработки и усовершенствования
	Защита компьютерных систем от СДВ по сетям питания	
6.	На все фидеры, выходящие за пределы контролируемой службой безопасности (СБ) зоны, установить групповые устройства защиты (ГУЗ) от СДВ	ГУЗ установить в зонах, подконтрольных СБ
7.	На сеть электропитания серверов, систем охраны и сигнализации объекта установить индивидуальную защиту	В зависимости от решаемых задач объем индивидуальной защиты может быть существенно расширен
8.	Щитки питания, распределительные щиты, розетки, клеммы заземления и т.п. необходимо размещать в помещениях, контролируемых СБ	Не рекомендуется установка розеток в слабо контролируемых помещениях (буфет, склад, гардероб и т.п.)
9.	Используя анализатор неоднородности линии снять контрольный "портрет" электросети.	Контрольный "портрет" снимается после завершения монтажа сети
10.	Для выявления несанкционированного подключения к сети необходимо регулярно контролировать текущий "портрет" электросети и сравнивать его с контрольным "портретом".	Этот метод контроля особенно эффективен для обнаружения ТС СДВ последовательного типа
11.	Доступ к щитам питания и другим элементам электрооборудования должен быть ограничен	Ограничение определяется соответствующими документами и мероприятиями
12.	Все электрооборудование, в том числе и бытового назначения, должно тщательно проверяться	Особое внимание обратить на ИБП, микроволновые печи, пылесосы, кондиционеры, аппараты для сварки

Табл. 2. Основные рекомендации по защите компьютерных систем от СДВ.

13.	Организовать круглосуточный мониторинг сети электропитания с одновременной записью в журнале всех сбоев и повреждений оборудования, фиксацией времени сбоев и характера дефектов. Путем анализа результатов возможно своевременное обнаружение факта НСД	В качестве регистраторов можно использовать широкий спектр приборов от простых счетчиков импульсов до комплексов с ПК
14.	При закупке электрооборудования необходимо обращать внимание на степень его защиты от импульсных помех. Обычное оборудование должно иметь класс устойчивости не ниже А, ответственное- не ниже В	По стандарту IEEE 587-1980 помеха класса А: 0,5 мкс/6 кВ/200 А/1,6 Дж; класса В: 0,5 мкс/6 кВ/500 А/4 Дж
15.	Для защиты 1-го рубежа лучше всего подходят специально разработанные помехозащищенные трансформаторные подстанции и суперфильтры. Класс защиты должен быть выше В, т.е. устройство защиты должно быть рассчитано на воздействие индуцированных напряжений от близких разрядов молний с возможным импульсным током до 40 кА	Автоматические устройства переключения сети не защищают от СДВ из-за низкого быстродействия. Также малопригодны тиристорные стабилизаторы и корректоры
16.	Для защиты 2-го рубежа могут использоваться технические средства с меньшим запасом энергии, в том числе суперфильтры, корректоры напряжения и помехоподавляющие трансформаторы	Суперфильтры, помимо специальных фильтров и ограничителей напряжения, могут содержать адаптивные схемы поглощения энергии СДВ
17.	Для защиты 3-го рубежа наиболее оптимальными являются помехоподавляющие трансформаторы (трансфильтры) или сочетание корректора напряжения, ограничителя и фильтра. Трансфильтр гораздо эффективней остальных типов фильтров и корректоров напряжения	Современные конструкции трансфильтров обеспечивают работоспособность компьютера при воздействии мощной импульсной помехи с амплитудой **до 10 кВ (!)**
Защита компьютерных систем от СДВ по проводным линиям		
18.	На все проводные линии связи и аварийно-охранно-пожарной сигнализации, которые выходят за пределы зоны контроля службы безопасности, установить устройства защиты от СДВ	Места для установки шкафов с УЗ выбираются в зонах, подконтрольных службе безопасности
19.	Для выявления несанкционированного подключения к проводным линиям с помощью анализатора неоднородности снять контрольный "портрет" сети. Систематическое сравнение текущего и контрольного "портретов" сети обеспечивает обнаружение НСД	Контрольный "портрет" снимается только после полного завершения монтажа сети проводных линий
20.	Доступ к линиям связи и сигнализации, датчикам, кросс-панелям, мини-АТС и другим элементам системы безопасности должен быть ограничен	Ограничение обеспечивается соответствующими документами и техническими средствами
21.	Нежелательно размещение оборудования сети (маршрутизаторов, АТС, кросса и т.п.) на внешних стенах объекта	В этом случае велика вероятность успешного СДВ из неконтролируемой зоны
22.	Желательно не применять общепринятую топологию прокладки проводных линий связи и сигнализации вдоль стены параллельно друг другу, т.к. она является идеальной для атаки на объект с помощью ТС СДВ с бесконтактным емкостным инжектором. Целесообразно использовать многопарные кабели связи с витыми парами	В противном случае с помощью плоского накладного электрода и ТС СДВ оборудование может быть выведено из строя злоумышленником за 10-30 с
23.	При закупке оборудования необходимо учитывать степень его защиты от импульсных помех. Минимальная степень защищенности должна соответствовать ГОСТ Р 50746-95 при степени жесткости испытаний 3-4	Амплитуда испытательного импульса должна быть 1 кВ для 3 степени и ли 2 кВ для 4 степени испытаний
24.	Для защиты 1-го рубежа необходимо установить защиту всех проводных линий от перенапряжений с помощью воздушных разрядников и варисторов. Кабели связи и сигнализации необходимо экранировать с использованием металлорукавов, труб и коробов.	Защита устанавливается как между линиями связи, так и между каждым из проводников и контуром заземления
25.	Для защиты 2-го рубежа можно использовать комбинированные низкопороговые помехозащитные схемы из таких элементов, как газовые разрядники, варисторы, комбинированные диодные ограничители, RC- и LC- фильтры и другие элементы.	Желательно установить групповое устройство защиты, выполненное в виде шкафа с замком
26.	Для защиты 3-го рубежа необходимо применять схемы защиты, максимально приближенные к защищаемому оборудованию	Схемы защиты 3 рубежа обычно интегрируются с разъемами, розетками, компьютерами и т.п.
Защита компьютерных систем от электромагнитного СДВ по эфиру		
27.	Основным методом защиты от СДВ является **экранирование** на всех рубежах как аппаратуры, так и помещений. При невозможности экранирования всего помещения необходимо прокладывать линии связи и сигнализации в металлических трубах или по широкой заземленной полосе металла., а также использовать специальные защитные материалы	В качестве экранирующего материала можно использовать металл, ткань, защитную краску, пленку, специальные материалы

Табл. 2 (продолжение). Основные рекомендации по защите компьютерных систем от СДВ.

28.	Многорубежная защита от СДВ по эфиру организуется аналогично защите по сети питания и по проводным линиям	См. пп 15-17, 25-27
29.	Вместо обычных каналов связи использовать, по возможности, волоконно-оптические линии	Использование волоконно-оптических линий защищает также от возможной утечки информации
30.	В защищенных помещениях особое внимание обратить на защиту по сети питания, используя, в первую очередь, разрядники и экранированный кабель питания	Обратить внимание, что традиционные фильтры питания от помех здесь не спасают от СДВ
31.	Учесть необходимость устранения любых паразитных излучений как защищаемой, так и вспомогательной аппаратуры объекта	Излучения не только демаскируют аппаратуру, но и способствуют прицельному наведению электромагнитных ТС СДВ
32.	Персоналу службы безопасности необходимо учитывать, что СДВ по эфиру организуется, как правило, из неконтролируемой зоны, в то время как его деструктивное действие осуществляется по всей территории объекта	Расширение зоны контроля службы безопасности возможно за счет использования телевизионного мониторинга за пределами объекта

Табл. 2 (окончание). Основные рекомендации по защите компьютерных систем от СДВ.

ки мегаджоулей, причем уровень пиковой мощности достигал десятков тераватт. Упрощенная схема такого генератора с взрывным сжатием магнитного поля приведена на рис. 7.

Как видно из рисунка, основу генератора с взрывным сжатием магнитного поля составляет цилиндрическая медная трубка с взрывчатым веществом, выполняющая функции ротора. Статором генератора служит спираль из медного провода, окружающая роторную трубку. Первоначальное магнитное поле в генераторе формируется стартовым током из любого внешнего источника, способного обеспечить импульс электрического тока силой от нескольких килоампер. Подрыв взрывчатки происходит с помощью специального генератора в момент, когда ток в статорной обмотке достигает максимума. Образующийся при этом плоский фронт взрывной волны распространяется вдоль взрывчатки, деформируя роторную трубку и превращая ее цилиндрическую форму в коническую (пунктир на рисунке). В момент расширения трубки до размеров статора происходит короткое замыкание статорной обмотки, приводящее к эффекту сжатия магнитного поля и возникновению мощного импульса тока порядка нескольких десятков мегаампер. Увеличение выходного тока по сравнению со стартовым зависит от конструкции генератора и может достигать десятков раз. В настоящее время уже удалось довести пиковую мощность генераторов с взрывным сжатием магнитного поля до десятков тераватт [3]. Это говорит о высоких потенциальных возможностях практической реализации средств силового деструктивного воздействия.

4. Рекомендации по защите компьютерных систем от силового деструктивного воздействия

На основании полученных и рассмотренных выше результатов можно сформулировать рекомендации по защите компьютерных систем от СДВ, основные из которых приведены в табл. 2.

5. Заключение

Силовые деструктивные воздействия, реализуемые по проводным и беспроводным каналам, а также по сетям питания, в настоящее время являются серьезным оружием против компьютерных систем, интегрированных систем безопасности и др. Это оружие оправдывает свое название «электромагнитной бомбы» и по эффективности воздействия является более опасным, чем программное разрушающее оружие для компьютерных сетей. Новые технологии делают технические средства силового деструктивного воздействия все более перспективными для применения и требуют к себе большего внимания, в первую очередь, со стороны служб безопасности и разработчиков систем защиты. С этой целью в данной статье предложены организационные и технические меры, помогающие противостоять силовым деструктивным воздействиям.

6. Литература

1. Winn Schwartau. More about HERF than some? — Information Warfare: Thunder's month press, New York, 1996.
2. Carlo Kopp. The E-bomb — a Weapon of Electronical Mass Destruction. — Information Warfare: Thunder's Month Press, New York, 1996.
3. David A. Fulghum. Microwave Weapons Await a Future War. — Aviation Week and Space Technology, June 7, 1999.

О Руководстве по разработке профилей защиты на основе Общих критериев

Марк Кобзарь, Алексей Сидак
Центр безопасности информации

СОДЕРЖАНИЕ

1. Введение

В статье приводится обзор основных положений Руководства по разработке профилей защиты и заданий по безопасности, подготовленного Международной организацией по стандартизации (ISO) в развитие требований к Профилям защиты и Заданиям по безопасности, содержащихся в стандарте ISO/IEC 15408. Кроме того, в статье описаны назначение, структура и краткое содержание Руководства.

Принятие в июне 1999 года международного стандарта по критериям оценки безопасности информационных технологий (исторически сложившееся название — Общие критерии) [2-4] послужило мощным толчком к широкому использованию Общих критериев при разработке профилей защиты различных типов продуктов и систем информационных технологий (ИТ).

2. Понятие профиля защиты и его назначение

Общие критерии (ОК) представляют собой хорошо структурированную, универсальную библиотеку требований безопасности, сформулированных в весьма общем виде [1]. Их специализация и конкретизация осуществляется в двух основных конструкциях, определенных в ОК: профилях защиты (ПЗ) и заданиях по безопасности (ЗБ).

Профили защиты являются дальнейшим развитием классов защищенности Оранжевой книги и хорошо известных Руководящих документов (РД) Гостехкомиссии России. Но, в отличие от их жесткой классификационной схемы, число профилей защиты не ограничено. Они содержат более полный, целенаправленный и обоснованный набор требований безопасности, учиты-

вающий назначение, угрозы безопасности и условия применения объекта оценки (ОО).

Профиль защиты предназначен для сертификации средств защиты информации продуктов и систем ИТ и получения сопоставимых оценок их безопасности. Профили защиты служат также основой для разработки разделов требований безопасности информации (заданий по безопасности) в ТЗ (ТТЗ) на конкретные изделия ИТ.

В настоящее время в России готовится проект государственного стандарта на основе аутентичного перевода текста стандарта ISO/IEC 15408. Параллельно в ряде организаций ведется разработка профилей защиты продуктов и систем ИТ различного назначения.

В этих условиях необходима единая методология создания и использования подобных нормативных документов.

В известном смысле можно утверждать, что профили защиты важнее самого стандарта ISO/IEC 15408. Данный стандарт по сути является метасредством, инструментом, предназначенным для разработки нормативных документов, позволяющих оценивать средства безопасности определенных классов или информационные системы определенного назначения. Именно эти нормативные документы, а не сам стандарт, способны найти практическое применение, обеспечить соответствие законодательного и технического аспектов информационной безопасности.

Практически все выпущенные ранее РД Гостехкомиссии России (от классификации средств вычислительной техники до критериев оценки межсетевых экранов) целесообразно переформулировать в виде профилей защиты, параллельно актуализировав их (Руководящих документов) содержание. Новые РД, на наш взгляд, с самого начала должны разрабатываться на основе стандарта ISO/IEC 15408. Подобные шаги сделали бы перспективы вхождения России в международные системы сертификации, а также заключения соглашений о взаимном признании сертификатов вполне реальными. В свою очередь, наличие таких соглашений лучше соответствовало бы реальному положению дел в России в области информационных технологий вообще и информационной безопасности в частности.

3. Назначение, структура и краткое содержание Руководства

В силу перечисленных выше причин, появление проекта Руководства по разработке профилей защиты и заданий по безопасности (далее — Руководство) [5], в котором развиваются и разъясняются основные требования к Профилям и Заданиям, изложенные в стандарте ISO 15408, является весьма актуальным.

Руководство, прежде всего, адресовано тем, кто участвует в процессе разработки Профилей и Заданий. Оно, вероятно, будет полезно и для оценщиков, применяющих Профили и Задания на практике.

Рассматриваемый документ представляет собой детальное руководство по разработке различных частей Профилей и Заданий (изложенное в главах 1-11) и дает исчерпывающее представление об их взаимосвязи. Наиболее важные аспекты Руководства представлены в Приложении А в виде памятки, что в значительной степени облегчает знакомство и работу с документом. В приложениях приводятся примеры, иллюстрирующие применение Руководства.

Глава 1 посвящена целям и направленности Руководства. Глава 2 содержит краткий обзор ПЗ и ЗБ, который включает примерные оглавления и отображает предполагаемое содержание, а также потенциальных пользователей различных частей Профилей и Заданий. В этой главе также обсуждаются соотношение между ПЗ и ЗБ и проблемы, связанные с процессом их разработки.

В Главе 3 более глубоко рассматриваются описательные части Профилей и Заданий.

Следующие пять глав придерживаются структуры Профилей и Заданий, установленной в стандарте ISO 15408.

Глава 4 представляет собой руководство по определению безопасности окружения объекта оценки. Глава 5 служит руководством по определению и спецификации целей безопасности в соответствии со сформулированными ранее исходными «потребностями».

Глава 6 — это руководство по выбору и спецификации требований безопасности информационных технологий в ПЗ. В этой главе подробно описывается использование функциональных компонентов [3] и компонентов гарантии [4], а также компонентов, не предусмотренных ISO 15408, для обеспечения более точного определения требований безопасности ИТ.

Глава 7 представляет собой руководство по разработке заданий по безопасности.

Главы 8 и 9 являются руководствами по составлению и представлению разделов «Обоснование» в ПЗ и ЗБ.

В главе 10 рассматриваются проблемы разработки ПЗ и ЗБ для сложных объектов оценки, то есть объектов, состоящих из двух или более компо-

нентов, для каждого из которых имеются собственные Профили и Задания.

Глава 11 представляет собой руководство по формированию функциональных пакетов и пакетов гарантии, причем таким образом, чтобы их можно было многократно использовать при разработке различных Профилей и Заданий. Пакет при этом рассматривается как потенциально полезный инструмент, предназначенный для облегчения процесса разработки ПЗ/ЗБ.

Как упоминалось выше, Приложение А резюмирует Руководство в виде памятки.

Приложение В представляет примеры угроз, политики безопасности организации, предположений и целей безопасности, а также устанавливает соответствие между общими функциональными требованиями и соответствующими функциональными компонентами из Части 2 стандарта ISO 15408 [3].

Приложение С представляет собой руководство по разработке ПЗ и ЗБ объектов оценки, обладающих криптографическими функциональными возможностями.

В Приложениях D, E и F иллюстрируются возможности применения Руководства при разработке ПЗ и ЗБ для различных объектов оценки. Так, в Приложении D рассмотрена возможность использования Руководства применительно к межсетевым экранам.

В Приложении E рассмотрен подход к разработке ПЗ для СУБД. Здесь особое внимание обращается на взаимодействие СУБД с операционной системой, под управлением которой она работает.

Наконец, Приложение F посвящено вопросам разработки Профилей для доверенного центра (ДЦ), являющегося центральным звеном в инфраструктуре с открытыми ключами и организующего работу с цифровыми сертификатами [6]. В Руководстве предлагается интересный подход к формированию ПЗ и ЗБ для ДЦ, учитывающий множество возможных комбинаций дополнительных услуг, предоставляемых конкретным ДЦ, наряду с неизменным набором основных услуг. Подход предусматривает формирование базового набора функциональных требований безопасности, необходимых для обеспечения безопасности основных услуг ДЦ, и дополнительных функциональных пакетов.

4. Заключение

В настоящее время в России и других странах СНГ Общим критериям уделяется много внимания. Пишутся статьи, готовятся к публикации книги. Хотелось бы, чтобы внедрение и освоение нового международного стандарта не стало формальной процедурой, не подкрепленной реальными изменениями в системах сертификации и аттестации. На наш взгляд, принятие Общих критериев должно стать первым звеном в цепи обновления нормативной базы информационной безопасности в России, освоения новых понятий разработчиками, оценщиками и пользователями информационных систем, движения России в сторону общепризнанных международных норм информационной безопасности.

Профили защиты — это применимые на практике результаты использования Общих критериев. Вот почему появление Руководства по разработке профилей защиты и заданий по безопасности представляется весьма важным, а его освоение — абсолютно необходимым.

5. Литература

1. Кобзарь М., Калайда И. Общие критерии оценки безопасности информационных технологий и перспективы их использования. — Jet Info, 1998, 1.
2. Evaluation Criteria for IT Security. Part 1: Introduction and general model. — ISO/IEC 15408-1: 1999.
3. Evaluation Criteria for IT Security. Part 2: Security functional requirements. — ISO/IEC 15408-2: 1999.
4. Evaluation Criteria for IT Security. Part 3: Security assurance requirements. — ISO/IEC 15408-3: 1999.
5. Guide for Production of Protection Profiles and Security Targets. — ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000.
6. Горбатов В., Полянская О. Доверенные центры как звено системы обеспечения безопасности корпоративных информационных ресурсов. Jet Info, 1999, 11.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su, http://www.jetinfo.ru
Подписной индекс по каталогу Роспечати **32555**