РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОТ ДЕСТРУКТИВНЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ

Царегородцев Анатолий Валерьевич,
Всероссийская государственная налоговая академия
Министерства финансов Российской Федерации (Москва)
05.13.19
academic_tsar@mail.ru

Аннотация. *Рассматриваются рекомендации по защите критически важных объектов, устойчивых по отношению к внешним преднамеренным электромагнитным воздействиям.*

Ключевые слова: информационная безопасность, деструктивное электромагнитное воздействие, защита, радиоэлектронное средство, экранирование.

RECOMMENDATIONS FOR INFORMATION OBJECTS PROTECTION FROM THE ELECTROMAGNETIC DESTRUCTIVE EFFECTS

Tsaregorodtsev Anatolii Valerievich
The State Tax Academy of Russian Federation (Moscow)

Abstract. *Recommendation for critical resistant protection to external intentional electromagnetic attacks is considered.*

Key words: information security, electromagnetic destructive effect, protection, radio electronic mean, screening.

Введение

С появлением возможности создавать малое по объему оборудования, которое может использоваться для генерирования коротких, интенсивных электромагнитных импульсов, возникла опасность электромагнитного терроризма. Проблема электромагнитного терроризма возникла не на пустом месте. Она обусловлена логикой развития двух, казалось бы, различных научных дисциплин – сильноточной электроники больших мощностей и твёрдотельной микроэлектроники – основы современной вычислительной техники и информатики. Не секрет, что сегодня размеры многих микроэлектронных устройств уменьшились до десятых долей микрометра, а сила тока – до микроампер. Последнее обстоятельство снижает порог разрушения микроэлектронных устройств, делая их весьма уязвимыми для средств поражения, использующих сильноточные генераторы электромагнитного излучения больших мощностей. Эта простая логика и привела к появлению нового вида оружия – электромагнитного оружия.

Электромагнитный терроризм (ЭМ-терроризм) является намеренным (злонамеренным) генерированием электромагнитной энергии, которая в виде шума или сигналов внедряется в электрические и/или электронные системы для террористических или преступных целей, приводя к нарушению функционированию или повреждению этих систем. ЭМ-терроризм может расцениваться как один из типов наступательной информационной войны. Электромагнитный терроризм требует рассмотрения и учета при комплексной безопасности критически важных объектов информатизации (КВОИ).

Электронные компоненты, типа микропроцессоров, работают на все более и более высоких частотах и с более низкими напряжениями и, таким образом, все более и более восприимчивы к электромагнитным возмущениям. Одновременно, наблюдается значительный прогресс в развитии радиосистем, совершенствовании их антенн, увеличении разнообразия оборудования, способного

к генерированию очень коротких радиоимпульсов, которые могут разрушать сложную электронику системы телекоммуникаций.

ЭМ-терроризм может быть привлекателен для злоумышленников, потому что он может быть предпринят тайно, анонимно и на некотором расстоянии от физических барьеров (систем охраны периметров, стен). Он может охватывать большое число целей и оставлять незначительные следы или действовать бесследно.

Оружие или устройства могут быть двух основных типов. Это могут быть микроволновые устройства высокой мощности, генерирующие мощные излучения в узкой полосе частот, которые могут вызывать существенные повреждение, или устройства, которые работают в широкой полосе. Подобные устройства наиболее вероятно вызовут сбой, если не серьезное повреждение. Поскольку интенсивность электромагнитного поля уменьшается пропорционально квадрату расстояния, то главный фактор, который следует принимать во внимание - расстояние между оборудованием и потенциальным источником опасности.

Важно, чтобы проектировщики электронных и телекоммуникационных систем, работающих в критических приложениях, знали потенциальные угрозы и принимали адекватные методы предотвращения риска злонамеренных повреждений. Проектировщик должен знать проблему, оценивать риски, связанные с проектируемым оборудованием или его использованием, и принимать соответствующие встречные меры. Каждый случай, где предварительно не рассматривалась проблема терроризма, может стать привести к угрозе террористического шантажа или другого злонамеренного ущерба.

1. Основные каналы деструктивного воздействия на объекты информатизации и рубежи защиты

Современные технические средства силового деструктивного воздействия (СДВ) являются по существу электромагнитным оружием, которое способно дистанционно и без лишнего шума поразить практически любую систему безопасности. Главное в этом случае - обеспечить соответствующую мощность электромагнитного импульса. Проведенный анализ показывает, что компьютер или любое другое электронное оборудование системы безопасности с учетом среды передачи энергии деградации могут быть подвергнуты силовому деструктивному воздействию по трем основным каналам силового деструктивного воздействия (КСДВ): по сети питания (КСДВ 1); по проводным линиям (КСДВ 2); по эфиру с использованием мощных коротких электромагнитных импульсов (КСДВ 3).

Основные каналы деструктивного воздействия на интегрированную систему безопасности и рубежи защиты приведены на рисунке 1.

Как видно из рисунка 1, использование СДВ, в принципе, позволяет преодолеть все стандартные рубежи защиты в ИСБ. Все определяется мощностью воздействия, выбранными средствами защиты, имеющимися финансовыми возможностями. Эти обстоятельства определяют выбор стратегии защиты.

Рассмотрим одну из них – двухуровневую стратегию защиты (ДСЗ).

При ДСЗ на первом (внутреннем) уровне предусматривается выбор соответствующих технических средств и постоянное тестирование их устойчивости на соответствие нормативным документам. На втором (внешнем) уровне предусматриваются организационно-технические мероприятия, направленные на максимально возможное ослабление или блокирование сигналов от СДВ (в частности, за счет экранирования).

2. Осуществление силовых деструктивных воздействий по сети электропитания

Для осуществления СДВ по сетям электропитания используется 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 электропитания, для чего, в первую очередь, необходимо провести классификацию технических средств СДВ. Однако, учитывая специфическое назначение данных средств и нежелание фирм их производящих широко афишировать свою работу, задача классификации оказалась не тривиальной. Возможная классификация современных технических средств СДВ по сетям электропитания, проведенная по результатам анализа, представлена на рисунке 2.

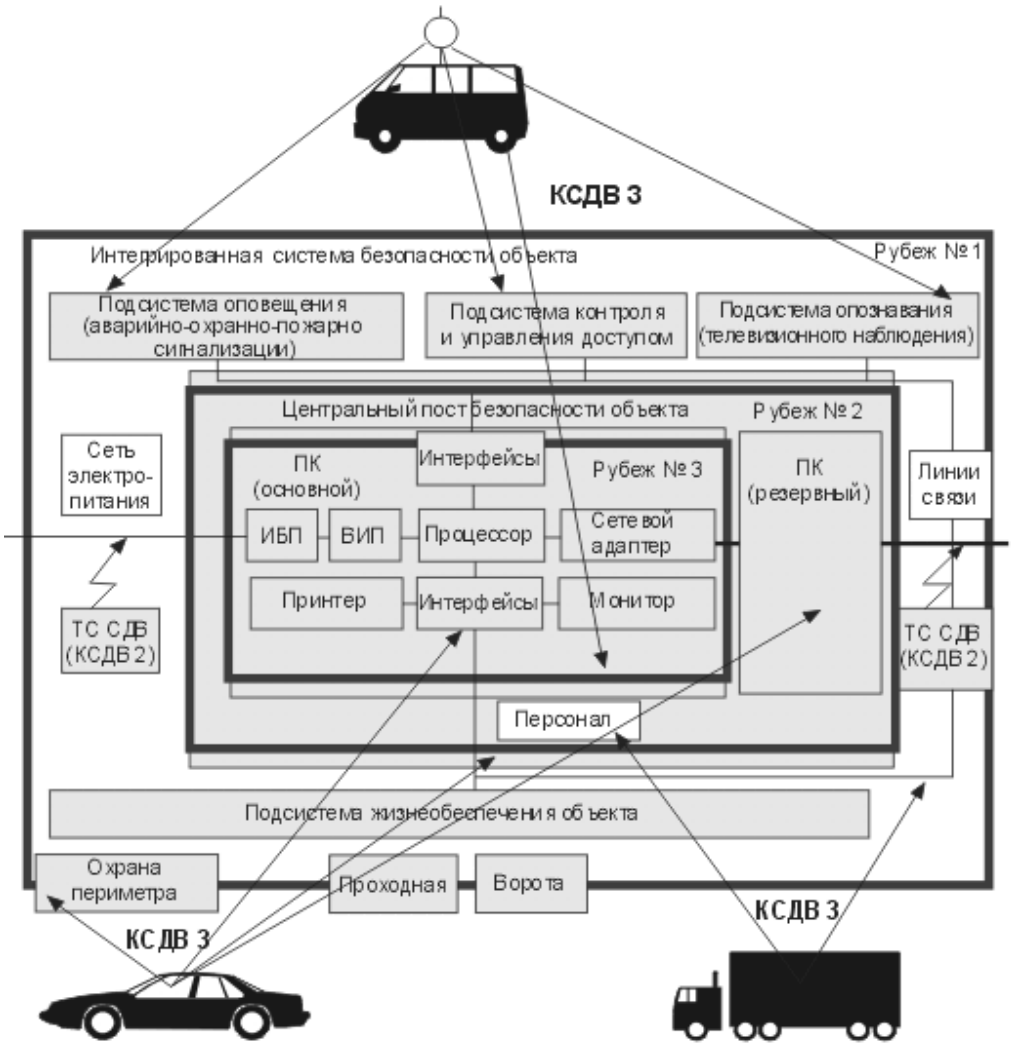

Рис. 1. Основные каналы деструктивного воздействия на интегрированную систему безопасности и рубежи защиты.

Таблица 1

Рекомендации по защите систем безопасности от СДВ

Рекомендация по защите систем безопасности от СДВ	**Примечание**
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
Произвести разделение объекта на зоны защиты и рубежи обороны: • 1 рубеж – защита по периметру объекта; • 2 рубеж – защита поэтажная: • 3 рубеж – индивидуальная защита	Для небольших объектов (офисов) 1 рубеж может отсутствовать, а 2 рубеж сократиться до защиты отдельного помещения
После проведения монтажа системы безопасности провести тестирование на реальные воздействия	Для тестирования используются специальные имитаторы СДВ
Разработать соответствующие документы ограничительного характера, направленные на ограничение возможности использования технических средств СДВ	Например, запретить использование розеток выделенной сети для пылесосов и другого оборудования, в которые могут быть встроены ТС СДВ и др.

Рис. 2. Классификация технических средств СДВ по сетям электропитания.

Отдельно стоит остановиться на исследовании класса «Специальные и другие ТС СДВ». К этому классу отнесены, в частности, различные суррогатные технические средства (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 источников бесперебойного питания (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 настоящее время для проникновения энергии СДВ по сети питания имеется два основных канала:

1) кондуктивный путь через вторичный источник питания (ВИП);
2) наводки через паразитные емкостные и индуктивные связи, как внутренние, так и внешние (например, через сигнальные цепи и линии связи), причем, по особенностям схемотехники каналы воздействия могут быть как симметричные, так и несимметричные.

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 ТС СДВ необходима энергия 50…100 Дж, амплитуда – 1 кВ, длительность импульса – 0,1 с.

Для вывода из строя конденсаторов входного фильтра инвертора и диодов моста 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. 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 воздействии весьма вероятен выход из строя транзисторов и других элементов инвертора, а также проход деструктивных импульсов на выход ВИП, что приведет к повреждению других узлов системы безопасности.

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 оборудования (например, компьютеров) имеют емкостную связь через паразитную емкость, равную 10…30 пФ, а паразитная емкость, равная 5… 10 пФ, связывает сеть питания с элементами материнской платы компьютера. 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 накладывают дополнительные требования к защите от импульсных помех.

По результатам анализа можно сделать вывод, что традиционные ВИП недостаточны для защиты компьютеров и технических средств безопасности от СДВ. Однако, между сетью питания и ВИП, как правило, устанавливается дополнительное устройство защиты (ИБП UPS, стабилизатор, фильтр, сетевой кондиционер и т.п.), которое необходимо также учитывать при оценке устойчивости к СДВ. В системах безопасности особенно широко в последнее время стали применяться источники бесперебойного питания UPS (Uninterruptible Power Supply), на которых необходимо остановиться особо. Эти устройства предназначены для улучшения качества энергии сети переменного тока и обеспечения бесперебойного электропитания оборудования при выходе из строя электросети.

По способу управления UPS разделяются на OFF-LINE и ON-LINE типы. Главное различие заключается в выборе основного канала передачи энергии к потребителю.

Для режима OFF-LINE в основном режиме переключатель каналов подключает вход UPS 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.

Режим ON-LINE характеризуется постоянством включения ветви, содержащей мощное зарядное устройство, аккумулятор и инвертор на выход блока UPS. 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 так же при разряде аккумуляторов, переключатель каналов подключает ветвь, соединяющую вход-выход через фильтр. Этот вспомогательный путь передачи энергии, получивший название байпас (BY PASS), имеет особое значение при СДВ и позволяет обойти защиту UPS для поражения более важных блоков системы безопасности, например, компьютера.

В последнее время появились линейно-интерактивные (line interactive) UPS, которые являются дальнейшим развитием технологии off-line. Они отличаются наличием на входе стабилизирующего автотрансформатора, что способствует стабилизации выходного напряжения UPS. В некоторых случаях, если допустимы перерывы в питании на несколько миллисекунд, линейно-интерактивные UPS оказываются предпочтительнее типа off-line и дешевле on-line устройств.

Обычно при СДВ по сети питания UPS выходит из строя, причем в этом случае срабатывает байпас и через него энергия ТС СДВ достигает цели в обход UPS. 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 от СДВ системы безопасности, но и сами весьма подвержены деструктивному воздействию. Основные рекомендации по защите систем безопасности от СДВ по сети электропитания приведены в таблице 2.

Таблица 2

Основные рекомендации по защите систем безопасности от СДВ по сети электропитания

Рекомендация по защите систем безопасности от СДВ	Примечание
На все фидеры, выходящие за пределы контролируемой службой безопасности (СБ) зоны, установить групповые устройства зашиты (УЗ) от СДВ	Групповые УЗ установить в зонах, подконтрольных СБ
На сеть электропитания серверов, систем охраны и сигнализации объекта установить индивидуальную защиту	В зависимости от решаемых задач объем индивидуальной защиты может быть существенно расширен
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.)
Используя анализатор неоднородности линии, снять контрольный «портрет» электросети	Контрольный «портрет» снимается после завершения монтажа сети
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
Текущее обслуживание и ремонт электрооборудования должны проводиться под контролем сотрудников службы безопасности	
Доступ к щитам литания и другим элементам электрооборудования должен быть ограничен	Ограничение определяется соответствующими документами и мероприятиями
Все электрооборудование, в том числе, и бытового назначения, должно тщательно проверяться	Особое внимание обратить на UPS, микроволновые печи, пылесосы, кондиционеры, аппараты для сварки
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
При закупке электрооборудования систем безопасности 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
Для защиты 1 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
Для защиты 2 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
Для защиты 3 рубежа наиболее оптимальными являются помехоподавпяющие 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

3. Осуществление силовых деструктивных воздействий по проводным слаботочным цепям

Классификация ТС СДВ по проводным линиям приведена на рисунке 3.

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, т.к. время пробоя МОП-структуры или pn-перехода составляет 10 – 1000 нс. Как известно, напряжения пробоя переходов составляют от единиц до десятков вольт. Таким образом, 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. В частности, в данном случае для СДВ может быть использован любой электромагнитный шокер.

Основные рекомендации по защите систем безопасности от СДВ по проводным линиям приведены в таблице 5.

Рис. 3. Классификация технических средств СДВ по проводным слаботочным линиям.

Таблица 3

Основные рекомендации по защите систем безопасности от СДВ по проводным линиям

Рекомендация по защите систем безопасности от СДВ	Примечание
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
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
Ремонтные работы и текущее обслуживание оборудования, линий связи и цепей сигнализации системы безопасности необходимо производить под контролем службы безопасности	
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

Рекомендация по защите систем безопасности от СДВ	Примечание
Нежелательно размещение оборудования сети (маршрутизаторов, ТС, кросса и т.п.) на внешних стенах объекта	В этом случае велика вероятность успешного СДВ из неконтролируемой зоны
Желательно не применять общепринятую топологию прокладки проводных пиний 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
При закупке оборудования систем безопасности необходимо учитывать степень его защиты от импульсных помех. Минимальная степень защищенности должна соответствовать ГОСТ Р 50746-95 при степени жесткости испытаний 3-4	Для более подробной информации см. журнал «Конфидент. Защита информации», N9 2, 1998
Для защиты 1 рубежа необходимо установить защиту всех проводных пиний от перенапряжений с помощью воздушных разрядников и заристоров. Кабели связи и сигнализации необходимо экранировать с ипользованием метэллоруковов, труб и коробов.	Защита устанавливается как между линиями связи, так и между каждым из проводников и контуром заземления
Для защиты 2 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
Для защиты 3 рубежа необходимо применять схемы защиты, максимально приближенные к защищаемому оборудованию	Схемы защиты 3 рубежа обычно интегрируются с разъемами, розетками, компьютерами и т.п.

4. Осуществление беспроводных силовых деструктивных воздействий

Наиболее скрытым и наиболее эффективным является канал силового деструктивного воздействия по эфиру с использованием мощного короткого электромагнитного импульса. В этом случае стало возможным реализовать достаточно компактные электромагнитные технические средства СДВ, размещаемые за пределами объекта атаки и на достаточном для маскировки атаки удаления от коммуникаций. Конструкция электромагнитного ТС СДВ на примере генератора с виртуальным катодом (виркатора) приведена на рисунке 4.

Как видно из рисунка 4, принцип работы виркатора заключается в следующем. При подаче на анод положительного потенциала порядка 105 – 106. 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 тормозиться 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.

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 сигнал (ЭМС) 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 понятие «электромагнитной бомбы».

Анализ показывает, что наиболее опасными ТС СДВ для интегрированных систем безопасности

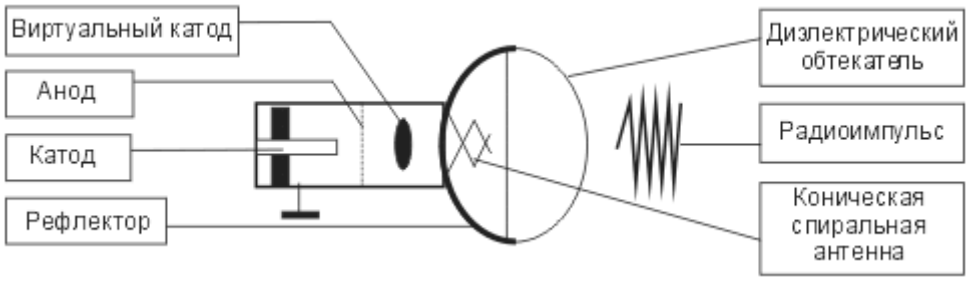

Рис. 4. Конструкция ЭМ ТС СДВ на примере виркатора.

являются технические средства силового деструктивного воздействия по эфиру с использованием электромагнитного импульса (беспроводные ТС СДВ). Особенно 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 беспроводных ТС СДВ, использованная в данной работе, приведена на рисунке 5.

Несмотря на то, что статистика использования СДВ сегодня не ведется (как правило, инциденты списываются на природные катаклизмы, такие как гроза, статика, случайные совпадения и т.п., и идентифицировать их очень сложно), вероятность использования СДВ сегодня весьма велика. Поэтому проблема защиты от СДВ, являясь весьма актуальной, требует своего решения. Основные рекомендации по защите систем безопасности от электромагнитного СДВ по эфиру приведены в таблице 4.

Рис. 5. Классификация беспроводных ТС СДВ.

Таблица 4

Основные рекомендации по защите систем безопасности от электромагнитного СДВ по эфиру

Рекомендация по защите систем безопасности от СДВ	Примечание
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
Многорубежная защита от СДВ по эфиру организуется аналогично защите по сети питания и по проводным линиям	
Вместо обычных каналов связи использовать, по возможности, волоконно-оптические линии	Использование волоконно-оптических линий защищает также от возможной утечки информации
В защищенных помещениях особое внимание обратить на защиту по сети электропитания, используя, в первую очередь, разрядники и экранированный кабель питания	Обратить внимание, что традиционные фильтры питания от помех здесь не спасают от СДВ
Учесть необходимость устранения любых паразитных излучений как защищаемой, так и вспомогательной аппаратуры объекта	Излучения не только демаскируют аппаратуру, но и способствуют прицельному наведению беспроводных ТС СДВ
Персоналу службы безопасности необходимо учитывать, что СДВ по эфиру организуется, как правило, из неконтролируемой службой безопасности 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

Актуальность проблемы защиты от электромагнитного СДВ возрастает еще и потому, что в настоящее время некоторые исследовательские работы закончились разработкой опытных образцов информационного оружия. Так представляет 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 около 1 ГВт (напряжение 265 кВ, ток 3,5 кА) и обладает большими возможностями ведения информационной войны. Так в руководстве по его применению и техническому обслуживанию определена основная его характеристика: зона поражения – 800 м от устройства в секторе 24 градуса. Причем, важно отметить, что лицам с электронными стимуляторами сердца доступ к установке запрещен. Используя данную установку, можно эффективно стирать не только кредитные карточки, но и записи на магнитных носителях.

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, которая состоит из 144 твердотельных излучателей импульсов длительностью менее 1 нс с суммарной мощностью 1 ГВт. Данная система может устанавливаться на подвижных объектах. Даже рассмотренные примеры 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.

Заключение

Эффекты воздействия ЭМИ обычно многообразны и трудно предсказуемы. Пока неизвестны модели, адекватно описывающие реакцию сколь-нибудь сложного электронного устройства на облучение мощным ЭМИ, особенно - сверхширокополосным. Небольшие изменения, например, во взаиморас-

положении источника и цели, могут приводить к проявлению эффектов воздействия в различных электронных цепях цели вследствие реализации приема ЭМИ по различным лепесткам. Может также наблюдаться кумуляция эффектов и/или самопроизвольное восстановление некоторых схем спустя время, длительность которого изменяется от нескольких миллисекунд до часов и даже дней (так называемый эффект «временного ослепления»). Даже подтвержденная стойкость того или иного изделия, например к электромагнитному импульсу ядерного взрыва, не является гарантией его стойкости по отношению к ЭМИ иного частотного диапазона. Сложный характер поражений может обусловить и психологические проблемы.

Разработка методов обеспечения информационной безопасности критически важных объектов, устойчивых по отношению к внутрисистемным помехам и внешним преднамеренным электромагнитным воздействиям, становится крайне необходимой. В мировой практике такие методы пока не получили широкого распространения, что объясняется новейшими достижениями в области генерации и изучения сверхмощных широкополосных электромагнитных полей, сравнительно недавним появлением угроз электромагнитного терроризма, снижением чувствительности быстродействующих систем, наличием значительных по протяженности распределенных локальных сетей. Все это требует пересмотра традиционных подходов к обеспечению информационной безопасности критически важных объектов с учетом нового вида угроз безопасности - внешних преднамеренным электромагнитным воздействиям.

Список литературы

1. Акбашев Б.Б. Экранирующие системы зданий и помещений. – М.: Изд-во МИЭМ,2008. – 110 с.
2. Царегородцев А.В. Основные принципы обеспечения безопасности информационных систем критически важных объектов // Экономика, налоги и право. – М.: Изд-во ВГНА Минфина России, 2009. - №1. – С. 152-161.
3. Carlo Kopp. The E-bomb — a Weapon of Electronical Mass Destruction. — Information Warfare: Thunder's month press, New York, 1996.
4. David A. Fulghum. Microwave Weapons Await a Future War. — Aviation Week and Space Technology, June 7, 1999.