ЭЛЕКТРОМАГНИТНАЯ УГРОЗА: от мифа — к реальности

Одной их характерных тенденций нового века стало широкое внедрение средств информатизации в разнообразные сферы деятельности. В их числе — управление технологическими и бизнес-процессами, управление системами и средствами защиты от природных, техногенных и террористических угроз, мониторинг оперативной обстановки и кризисное реагирование, управление системами жизнеобеспечения, связи и телекоммуникаций, транспортом, банковской инфраструктурой и пр.

Владимир БОГДАНОВ
генеральный директор ФГУП «ЦентрИнформ», лауреат премии Правительства РФ, к. т. н.

Михаил ЖУКОВСКИЙ
начальник научно-исследовательского испытательного центра ФГУП «ЦентрИнформ», к. т. н.

Сергей ЛАРИОНОВ
начальник отдела научно-исследовательского испытательного центра ФГУП «ЦентрИнформ»

Владимир ЧВАНОВ
начальник отдела научно-исследовательского испытательного центра ФГУП «ЦентрИнформ», к. т. н.

Важность этих процессов и тяжесть последствий их нарушения выдвигают в разряд первоочередных проблему их защиты от дестабилизирующих факторов. Если учитывать прямую взаимосвязь между эффективностью упомянутых процессов и бесперебойностью функционирования обеспечивающих их средств информатизации, то именно эти средства становятся одними из основных предметов защиты как от природных и техногенных, так и от террористических угроз. К последним можно отнести не только «традиционные» силовые действия, от которых достаточно эффективно можно защитить с помощью современных технологий безопасности, но и сильные электромагнитные излучения (ЭМИ), осуществляемые преднамеренно и целенаправленно для уничтожения, искажения и блокирования информации, обрабатываемой, хранимой и передаваемой с помощью средств информатизации.

Изначально источником такого ЭМИ, оказывающего деструктивное воздействие на электронные системы, считался ядерный взрыв (ЯВ), в результате которого генерируется мощный электромагнитный импульс [1]. Это явление достаточно хорошо изучено как с точки зрения оценки воздействия ЭМИ ЯВ на аппаратуру, выработки подходов к ее защите от данного фактора, так и с точки зрения создания нормативной базы, которая подробно представлена в комплексе международных стандартов МЭК 61000. Признавая высокие деструктивные

свойства ЭМИ ЯВ, следует отметить крайне низкую в настоящее время вероятность возникновения данной угрозы, связанную с действующим более 40 лет запретом на испытания ядерного оружия, а также с прогрессом в области сокращения ядерных вооружений ведущих стран — членов «ядерного клуба». Однако мифичность угрозы ЭМИ стала стремительно таять с развитием новейших разработок в области создания сверхмощных генераторов сверхкоротких (субнаносекундных) импульсов (ГСКИ), предназначенных изначально для натурного моделирования ЭМИ ЯВ. Их первые образцы (ГСКИ на жидкостных и газовых разрядниках), появившиеся в конце 50-х годов, уже позволяли получать импульсы длительностью от сотен наносекунд до сотен пикосекунд с частотой повторения до 100 Гц. Достигнутые при этом напряженности электрического поля свыше 100 кВ/м позволяли испытывать на устойчивость к ЭМИ достаточно широкий спектр электронного оборудования, однако элементная база того времени существенно ограничивала возможности практического применения ГСКИ. Имея большие габариты и вес, они использовались в основном в качестве стационарных изделий исключительно в исследовательских целях.

Стремительное развитие полупроводниковой технологии привело к созданию в 90-х годах твердотельных генераторов, которые по таким параметрам, как импульсная мощность и длительность импульса, не уступали своим предшественникам и, в свою очередь, значительно превосходили последние по частоте следования импульсов, обладая при этом малыми габаритами и весом. Успехи в разработке малогабаритных твердотельных генераторов и управляемых антенных решеток позволили создавать ГСКИ, формирующие сверхкороткие импульсы с пиковой мощностью в десятки терраватт, что в значительной мере уподобляет их по параметрам ЭМИ ЯВ.

В открытой печати и в Интернете можно найти описание таких генераторов вплоть до принципиальных схем формирователей сверхмощных субнаносекундных импульсов. Там же имеется достаточно широкий перечень публикаций, свидетельствующих о деструктивных эффектах, создаваемых этими устройствами. В качестве иллюстрации результатов воздействий ГСКИ на информационные системы и средства, а также на оборудование безопасности и связи в табл. 1 приводятся некоторые опубликованные в открытой печати [2, 3, 4] экспериментальные данные, полученные ведущими в данной области российскими научно-исследовательскими учреждениями (ВНИИОФИ, МГИЭМ, МНИРИ, ОИВТ РАН г. Москва, ФГУП «ЦентрИнформ» г. Санкт-Петербург, ТУСУР г. Томск и др.).

При этом прослеживаются конкретные взаимосвязи между нарушениями «системного» характера, проявляющимися в виде прекращения, замедления, неправильности функционирования оборудования, сокращения перечня решаемых им задач и пр., и функциональными нарушениями, проявляющимися в виде возможных последствий нарушений обеспечиваемых им видов деятельности. Систематизированный перечень таких последствий представлен на рис. 1.

Анализ этих данных показывает, что по последствиям угроза электромагнитной атаки (ЭМА) во многом соизмерима с угрозой прямых террористических атак, а в ряде случаев проведение ЭМА является единственно возможным способом реализации силовых действий. Помимо этого ЭМА имеют ряд особенностей, «выгодно» отличающих их от традиционных способов нападения, а именно:

- возможность дистанционного воздействия на предметы атак, позволяющая успешно применять ГСКИ из-за пределов контролируемых зон объектов;
- отсутствие явных демаскирующих признаков проявления угрозы ЭМА;
- отсутствие явных демаскирующих признаков наличия средств электромагнитного нападения;
- возможность поэлементной доставки средств нападения на объект и их последующей сборки в непосредственной близости от предмета атаки;
- отсутствие в действующем законодательстве юридической основы, предусматривающей административную и уголовную ответственность за проведение ЭМА и др.

Эти факторы в ряде случаев могут служить аргументами для предпочтения выбора ЭМА в качестве основного способа проведения противоправных акций по отношению к «традиционным» способам, предусматривающим применение оружия и взрывчатых веществ. Кроме того, ГСКИ могут успешно применяться как вспомогательные средства, способствующие реализации основных угроз, например, для преодоления элементов систем охраны при проникновении на объект.

С другой стороны, нельзя отрицать тот факт, что для использования средств электромагнитного нападения необходимы соответствующая специальная квалификация и материальные возможности для их приобретения. И тем не менее, учитывая фактическую доступность ГСКИ для «продвинутого» нарушителя (стоимость может составлять от 20 000$ при варианте «Дипломат» до 500 000$ при мобильном варианте), возможность существенного превышения величины наносимого ими ущерба по отношению к их стоимости, превосходство по ряду параметров перед традиционными средствами нападения, а также явную неэффективность противодействия данной угрозе существующих методов и средств безопасности, возможность электромагнитного нападения на средства информатизации как разновидность террористической акции следует считать вполне реальной. Таким образом, малогабаритные полупроводниковые ГСКИ, обладая возможностью воспроизведения деструктивных эффектов, подобных ЭМИ ЯВ, высокой мобильностью и доступностью в приобретении, могут рассматриваться в качестве потенциальных средств электромагнитного нападения на средства информатизации объектов широкого предназначения.

Признаком озабоченности угрозой электромагнитного терроризма и необходимости поиска решений проблемы борьбы с ней на международном уровне стало образование

Табл. 1. *Результаты воздействий ГСКИ на информационные системы и средства, а также на оборудование безопасности и связи*

Вид информационной системы	Вид воздействия и последствия
Локальная вычислительная сеть	Зависание и перезагрузка компьютеров, обнуление базовых установок в системе ввода-вывода BIOS ПК, значительное снижение информационного трафика вплоть до его полной остановки при воздействии последовательности СКИ ЭМП с напряженностью электрического поля в точке воздействия 2–10 кВ/м, либо при инжектировании последовательности сверхкоротких электрических импульсов в цепь питания и линии связи
Средства связи и навигации	Уменьшение эффективной дальности связи до 2…10 раз, ложные показания либо зависание навигационного оборудования при воздействии СКИ ЭМП с напряженностью электрического поля в точке воздействия 1,5–3,0 кВ/м
Технические средства охраны	Зависания устройств считывания и контроллеров СКУД. Ложные срабатывания датчиков охранно-пожарной сигнализации. «Застывший кадр» телевизионных цифровых и Web-камер

Рис. 1. *Перечень возможных последствий нарушения функционирования средств информатизации*

в 1997 г. Комиссией E URSI отдельного подкомитета по электромагнитному терроризму в составе Комитета по ЭМИ и связанными с ним явлениями. Практически тогда же проблема защиты от электромагнитного терроризма сформировалась как самостоятельное направление в области электромагнитной совместимости (ЭМС). Ее решение поручено подкомитету 77C МЭК (председатель Уильям Радаски), который организовал, начиная с 1999 г., активную работу по созданию стандартов, направленных на обеспечение устойчивости гражданских объектов к действию мощных ЭМИ (напряженностью 100 кВ/м и более), предотвращение угрозы нерегламентированного применения неядерных источников мощных ЭМИ и безопасности человека. Применяя подходы и термины в области безопасности информационных технологий, изложенные в международном стандарте ИСО/МЭК 15408-1 (Общие критерии), угрозу

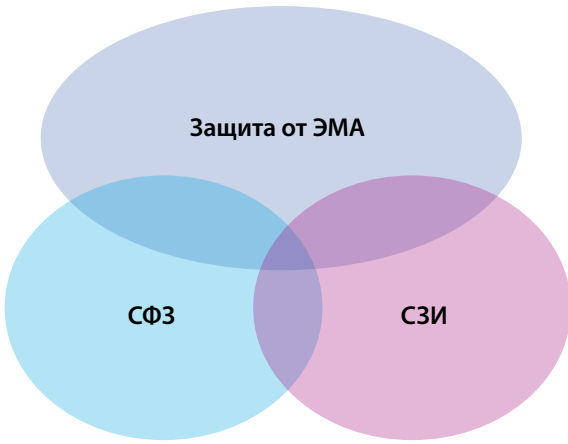

Рис. 2. *Взаимодействие защиты от ЭМА со штатными системами безопасности объекта*

преднамеренного электромагнитного воздействия (ПД ЭМВ) на информационную систему можно охарактеризовать как угрозу злоумышленных действий, направленных на уничтожение, искажение и блокирование информации.

Следуя рекомендациям международных стандартов, в России проводится активная деятельность в направлении создания соответствующей нормативной базы в виде Системы национальных стандартов по защите информации от преднамеренного электромагнитного воздействия. Эта работа ведется рабочей группой «Защита информации от специального воздействия», сформированной в составе Технического комитета по защите информации (ТК 362). В результате ее деятельности в период 2006–2007 г.г. в основополагающие стандарты по защите информации (ГОСТ Р 50922 и ГОСТ Р 51275) введен ряд ключевых понятий и определений по защите информации от преднамеренного силового электромагнитного воздействия (ПД ЭМВ). С июля 2008 года в России введен ГОСТ Р 52863 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования» [5] (головной разработчик — Санкт-Петербургский филиал ФГУП «НТЦ «Атлас», ныне — ФГУП «ЦентрИнформ»).

Дальнейшее развитие системы национальных стандартов предусматривает разработку в ближайшей перспективе общих положений в части организации работ по защите информации от ПД ЭМВ и общих требований, предъявляемых к средствам защиты и средствам обнаружения электромагнитных атак, а также требований к обеспечению контроля защищенности объектов от данной угрозы. Сформированная таким образом совокупность целевых стандартов регламентирует процессы создания и эксплуатации объектов в защищенном от ПД ЭМВ исполнении и устанавливает подходы к определению сбалансированного состава структурных компонент защиты от ЭМА и их характеристик. Это позволяет, в первую очередь, опре-

делить соответствующие ориентиры для целенаправленной деятельности по защите от данной угрозы на уровне ведомств, в составе которых эксплуатируются потенциально опасные и критически важные объекты. Кроме того, стандарты будут способствовать гармонизации взаимодействия различных профильных субъектов, участвующих в обеспечении безопасности информации и объектов. Упомянутые выше стандарты будут содержать много полезной информации для широкого круга специалистов в данной области, включая заказчиков и производителей систем безопасности.

Как показал предварительный анализ, эффективная защита от ЭМА не может быть обеспечена только путем повышения устойчивости к ПД ЭМВ самих средств информатизации. Являясь информационной по формальным признакам, угроза ЭМА фактически является силовой, и противодействие ей должно оказываться на всех стадиях проявления. Из этого следует, что защита от ЭМА должна быть комплексной, строиться с учетом объектовых условий и структурно интегрироваться и функционально дополнять штатные системы безопасности объекта, прежде всего, систему физической защиты (СФЗ) и систему защиты информации (СЗИ). Наглядное представление сфер взаимодействия указанных систем дается на рис. 2.

При таком подходе основная ответственность за защищенность объектов от ЭМА будет возлагаться на органы и службы безопасности объектов. В этом случае их внимание должно уделяться защите средств информатизации как основного, так и вспомогательного назначения, и, прежде всего, технических средств охраны (ТСО). Предназначенные для выполнения охранных функций и не обладающие достаточной устойчивостью к ПД ЭМВ ТСО не будут способны реализовывать свои высокие функциональные свойства при проведении против них электромагнитных атак. Этот факт должен привести к частичному пересмотру устоявшихся подходов к построению систем охраны объектов, начиная от предпроектной стадии, включая анализ уязвимости объекта и концептуальное проектирование СФЗ и последующие выбор типажа и порядка размещения технических средств охраны, а также разработку комплекса организационных мер защиты.

Помимо этого обязательным требованием, фигурирующим в проектах, разрабатываемых ГОСТ, является наличие данных об устойчивости к ПД ЭМВ для поставляемых на объект средств информатизации, в том числе ТСО. Их получение и последующая сертификация средств осуществляется на основе проведения испытаний согласно ГОСТ Р 52863-07. Этот процесс имеет ряд особенностей, требующих отдельного рассмотрения как в части методического, так и в части организационного обеспечения, которое будет проведено в последующих статьях.

Литература:

1. Н. В. Балюк, Л. Н. Кечиев, П. В. Степанов «Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты», изд. «Группа ИДТ», Москва, 2008

2. К. Ю. Сахаров, О. В. Михеев, О. В. Туркин, А. Н. Корнев, С. Н. Долбня, А. В. Певнев, Б. Б Акбашев «Исследование воздействия сверхкоротких электромагнитных импульсов на персональные компьютеры». Журнал «Технологии ЭМС», 2006, № 2

3. Л. О. Мырова, В. В. Воскобович «Воздействие сверхширокополосного электромагнитного излучения на технические средства». Журнал «Технологии ЭМС», № 3 (10), 2004

4. «Электромагнитный терроризм на рубеже тысячелетий» сборник статей под ред. Т. Р. Газизова, Томск, 2002

5. ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования».