Лекция 16. Сущность внешнего силового электромагнитного воздействия (СЭМВ) как угроза безопасности информации в АС

1.Эффекты, возникающие при внешнем ЭМВ на АС и СВТ. Основные каналы внешнего ЭМВ.

2. Требования устойчивости к преднамеренным внешним СЭМВ на информацию в АС.

3.Методы испытаний на устойчивость к предна-меренным внешним СЭМВ на информацию в АС.

1.Эффекты, возникающие при внешнем ЭМВ на АС и СВТ. Основные каналы внешнего ЭМВ.

СЭМВ – резкий всплеск напряжения в сетях питания, комму-никаций или сигнализаций систем безопасности с амплиту-дой, длительностью и энергией всплеска, способными приве-сти к сбоям в работе оборудования или к его полной деграда-ции.

Технические средства СЭМВ - ЭМ дистанционное оружие, способное дистанционно и без лишнего шума поразить лю-бую незащищенную систему безопасности мощным ЭМ им-пульсом.

ТС СЭМВ существенно повышают скрытность нападения то обстоятельство, что анализ повреждений в уничтоженном оборудовании не позволяет однозначно идентифицировать причину возникновения повреждения, так как причиной мо-жет быть как преднамеренное (нападение), так и непредна-меренное (например, индукция от молнии) силовое деструк-тивное воздействие. Это обстоятельство позволяет злоумы-шленнику успешно использовать ТС СЭМВ неоднократно.

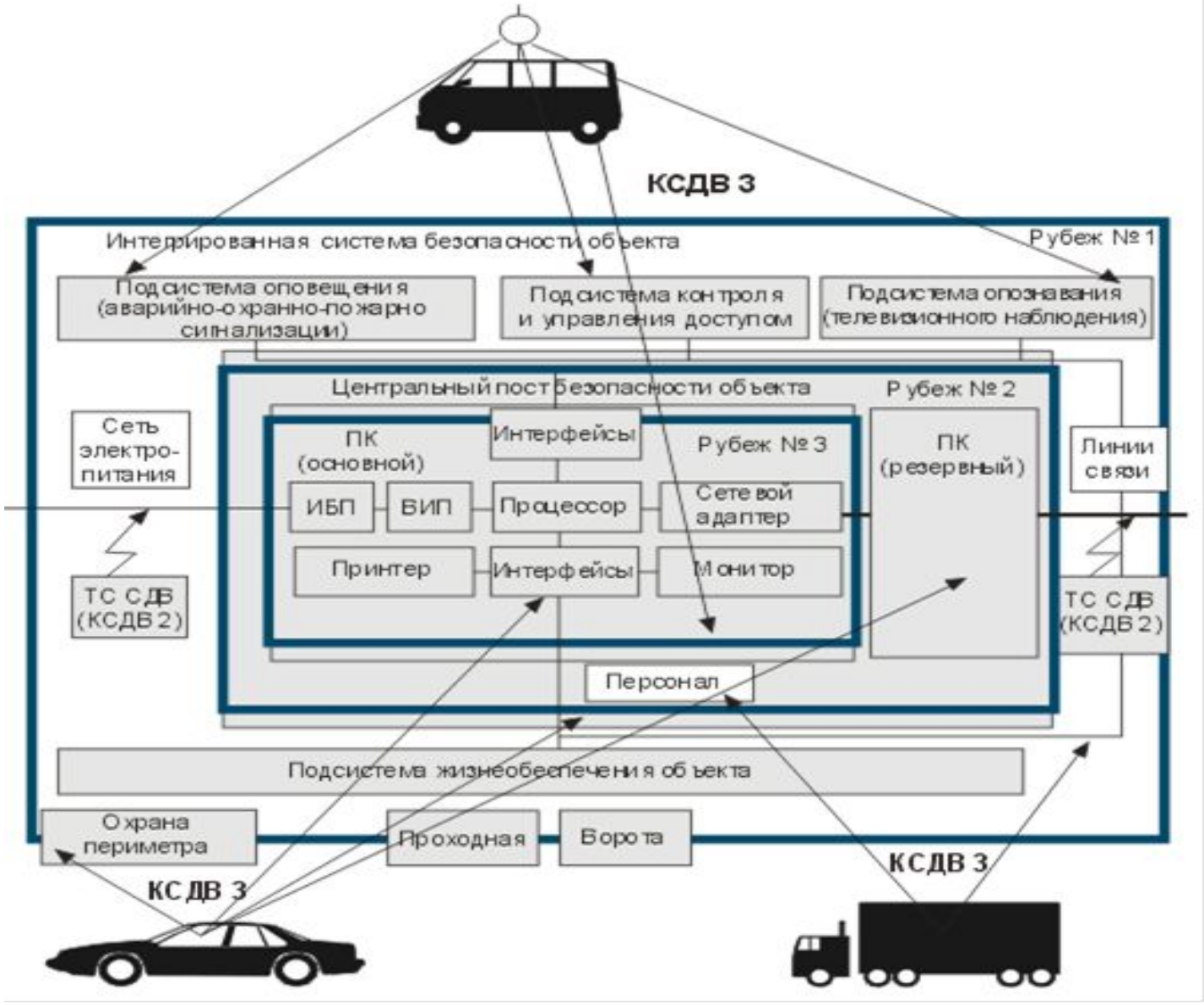
Вывод: Компьютер или любое другое электронное оборудование системы безопасности с учетом среды передачи энергии и деградации могут быть подвергнуты СЭМВ.

Известны три основных канала силового электромагнитного воздействия (КСЭМВ):

- по сети электропитания (КСЭМВ № 1);
- по проводным линиям (КСЭМВ № 2);
- по эфиру с использованием мощных коротких электромагнитных импульсов (КСЭМВ №3).

СЭМВ, в принципе, позволяет преодолеть все стандартные рубежи защиты в ИСБ АС. Это определяется мощностью воздействия, выбранными средствами защиты, имеющимися финансовыми возможностями.

Согласно ГОСТ Р 50922-2007, преднамеренное силовое ЭМ воз-действие на информацию является "несанкционированным воз-действием на информацию, осуществляемым путем применения источника электромагнитного поля для наведения (генерирова-ния) в автоматизированных информационных системах ЭМ энер-гии с уровнем, вызывающим нарушение нормального функцио-нирования (сбой в работе) технических и


КСДВ 3
Интегрированная система безопасности объекта
Рубеж №1
Подсистема оповещения (аварийно-охранно-пожарно сигнализации)
Подсистема контроля и управления доступом
Подсистема опознавания (телевизионного наблюдения)
Центральный пост безопасности объекта
Рубеж №2
Сеть электро-питания
ПК (основной)
Интерфейсы
Рубеж №3
ПК (резервный)
Линии связи
ИБП
ВИП
Процессор
Сетевой адаптер
Принтер
Интерфейсы
Монитор
ТС СДВ (КСДВ 2)
ТС СДВ (КСДВ 2)
Персонал
Подсистема жизнеобеспечения объекта
Охрана периметра
Проходная
Ворота
КСДВ 3
КСДВ 3

От традиционных угроз преднамеренное СЭМВ отличают:

•дистанционность воздействия - позволяет совершать акцию на некотором удалении от объекта воздействия, в том числе из-за пределов зоны его защиты от традиционных средств;

• "прозрачность" для ПД СЭМВ стандартных материалов строи-тельных конструкций (железобетон, кирпич), являющихся грани-цами охраняемых зон и помещений;

•компактность исполнения, отсутствие явных демаскирующих признаков средств ПД СЭМВ;

•возможность дистанционного управления (в том числе из-за пре-делов объекта) - позволяет распределять между разными испол-нителями функции доставки средства воздействия и его проведе-ние, выбирать наиболее критический с точки зрения последствий момент для совершения акции;

•отсутствие признаков совершения акции с помощью ПД СЭМВ, позволяющих оперативно определить причину возникновения нештатной ситуации и принять адекватные меры по недопущению (уменьшению) неконтролируемых и нежелательных последствий;

•возможность достижения цели акции путем ПД СЭМВ

2. Требования устойчивости к преднамеренным внешним СЭМВ на информацию в АС.

Требования устойчивости АСЗИ к преднамеренным СЭМВ относятся к техническим требованиям по защите информации по ГОСТ Р 51624, включающим требования:

1. к техническому обеспечению АСЗИ (основным и вспомогательным средствам);

1. к зданиям (помещениям) или объектам, в которых устанавливаются АСЗИ;

2. к программному обеспечению АСЗИ;

3. к средствам защиты информации и контроля эффективности защиты информации.

Требования к зданиям (помещениям) или объектам, в которых устанавливаются АСЗИ, включают требования к:

1. экранирующим свойствам ограждающих конструкций;

2. системе контроля и управления доступом;

3. системе сбора и обработки информации;

4.по устойчивости к взлому ограждающих конструкций;

5. дверным и оконным конструкциям;

6. замкам и запирающим конструкциям;

7.сейфам и хранилищам для носителей информации;

8.средствам защиты подходящих извне линий электроснабжения, проводных ЛС, заземления и т.п.

Требования к программному обеспечению включают требования к:

1.алгоритму принятия решения;
2.системе классификации;
3.системе команд;
4.алгоритму обработки событий;
5.по сертификации программного обеспечения;
6.системе диагностики программного обеспечения.

Требования устойчивости АСЗИ к ПД СЭМВ включают требования:

1. устойчивости к ПД СЭМВ по сети электропитания;
2. устойчивости к ПД СЭМВ по проводным линиям связи;
3. устойчивости к ПД СЭМВ по металлоконструкциям;
4. устойчивости к ПД СЭМВ электромагнитным полем.

К АСЗИ могут дополнительно предъявляться повышенные требования устойчивости к ПД СЭМВ , устанавливаемые стандартами по электромагнитной совместимости (ЭМС). Повышенные требования по стандартам ЭМС устанавли-ваются заказчиком для АСЗИ конкретного вида.

3. Методы испытаний на устойчивость к преднамеренным внешним силовым электромагнитным воздействиям на информацию в АС.

Таблица 1 - Степень жесткости испытаний АСЗИ при ПД СЭМВ электромагнитным полем

Класс условий эксплуатации	Степень жесткости испытаний ТС и объектов с АСЗИ				
	Технические средства	Системы обеспечения безопасности периметра объекта	Системы обеспечения безопасности объекта	Локальные выделенные сети и СКС	Помещения с ответственным оборудованием[2)]
Класс 5	I	IV	III	Не применяют[1)]	Не применяют[1)]
Класс 4	I	IV	III	II	II
Класс 3	I	IV	III	II	I
Класс 2	I	IV	III	II	I
Класс 1	I	IV	III	II	I
Класс 0	I	IV	III	II	I
Класс X	3)	3)	3)	3)	3)

[1)] Степень жесткости испытаний может быть введена специальными требованиями к АСЗИ.
[2)] В зданиях с кирпичными и деревянными стенами - все помещения. В зданиях с железобетонными стенами - только помещения, примыкающие к внешним стенам здания. В зданиях с металлическими стенами – только помещения с окнами.
[3)] Степень жесткости испытаний устанавливается специальными требованиями.

Степени жёсткости испытаний

Степени жёсткости испытаний, а также группу исполнения АСЗИ и объекта с АСЗИ по устойчивости к ПД СЭМВ выбирают исходя из условий эксплуатации оборудования и наличия специальных требований к АСЗИ. Данные условия определяются на основе анализа требований к условиям эксплуатации оборудования, класса информации, мощности выделенной сети электропитания ТС, мощности устройств защиты от преднамеренных силовых электромагнитных воздействий, степени экранирования помещений, в которых размещены ТС АСЗИ, степени защиты помещений от несанкционированного доступа, наличия систем охранной сигнализации, наличия специальных требований к АСЗИ.

Качественные признаки классификации типовых условий эксплуатации АСЗИ применительно к возможности воздействия с применением технических средств преднамеренных силовых электромагнитных воздействий приведены в приложении А.

Испытания на устойчивость к ПД СЭМВ электромагнитным полем

Испытание АСЗИ на устойчивость к ПД СЭМВ ЭМ полем проводятся для случаев возможного применения средств воздействия внутри и снаружи здания (соору-жения), в которых расположены АСЗИ или ее составные части.

Таблица 8 - Значения типовых параметров испытательных воздействий электромагнитным полем

№ п/п	Вид воздействия	Параметры испытательных воздействий	Степень жесткости испытаний			
			I	II	III	IV
1	Однократные наносекундные импульсы электромагнитного поля	Длительность импульса, нс	100	100	100	100
		Напряженность импульсного электрического поля, кВ/м	1	2	5	10
2	Периодические наносекундные импульсы электромагнитного поля с низкой частотой повторения	Длительность импульса, нс	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3
		Напряженность импульсного электрического поля, кВ/м	0,3	10	20	30
		Частота следования, кГц	1	1	1	1
3	Периодические наносекундные импульсы электромагнитного поля с высокой частотой повторения	Длительность импульса, нс	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3	0,2±0,1 0,8±0,3
		Напряженность импульсного электрического поля, кВ/м	0,02	0,02	0,2	0,2
		Частота следования, кГц	1000	1000	1000	1000

ЗАКЛЮЧЕНИЕ

Таким образом, ПД СЭМВ , реализуемое по проводным и беспро-водным каналам, а также по сетям питания, в настоящее время является серьезным оружием против систем защиты объектов АС, в частности, интегрированных систем безопасности и защищенных помещений. Это оружие оправдывает свое название “ЭМ бомбы” и по эффективности воздействия является более грозным, чем программное разрушающее оружие для компьютерных сетей. Аналитические исследования показывают, что новые технологии делают технические средства силового электромагнитного воздействия все более перспективными для применения и требуют к себе большего внимания, в первую очередь, со стороны служб безопасности и разработчиков систем защиты.