10.Гизатуллин З.М., Гизатуллин Р.М., Назметдинов Ф.Р., Набиев И.И. Повышение помехоустойчивости электронных средств при электромагнитных воздействиях по сети электропитания // Журнал радиоэлектроники: электронный журнал. – 2015. – №6.- С. 2.

11.Белоусов А.О., Газизов Т.Р., Заболоцкий А.М. Многопроводная микрополосковая линия как модальный фильтр для защиты от сверхкоротких импульсов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2015. – №3. – С. 124-128.

12. Газизов А.Т., Заболоцкий А.М., Газизов Т.Р. Разложение сверхкороткого импульса в структурах с лицевой связью // Известия высших учебных заведений. Физика. – 2017. – №3. – С. 70-75.

13. Белоусов А.О., Заболоцкий А.М., Газизов Т.Р. Экспериментальное подтверждение модельной фильтрации в многопроводной микрополосковой линии // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. – №3. – С. 51-54.

М.С. Шкиндеров, О.В. Чернов, Р.М. Гизатуллин

ФУНКЦИОНИРОВАНИЕ ЦИФРОВЫХ ЭЛЕМЕНТОВ ПРИ ПРЕДНАМЕРЕННОМ ВОЗДЕЙСТВИИ МИКРОСЕКУНДНЫХ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

Прогнозы специалистов показывают, что вероятность использования электромагнитного воздействия по сетям электропитания растет год от года [1, 2]. При этом сеть электропитания и так является хорошим переносчиком непреднамеренных электромагнитных помех [3, 4]. Поэтому при разработке концепции безопасности объекта, в частности включающего в себя систему контроля управления доступом (СКУД), необходимо учитывать и возможность преднамеренного электромагнитного воздействия по сетям электропитания [5, 6, 7, 8, 9]. Для осуществления электромагнитного террора 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.

Целью данной работы является анализ функционирования цифровых элементов электронных средств (ЭС), в частности СКУД, при преднамеренных электромагнитных воздействиях по сети электропитания при различных способах подключения генератора электромагнитных импульсов (ЭМИ) к сети. Известно о существовании следующих способов подключения генератора ЭМИ к сети питания: фазой и нейтралью; фазой и заземлением; нейтралью и заземлением. В данной работе рассматривается первые два способа (рис. 1, рис. 2).

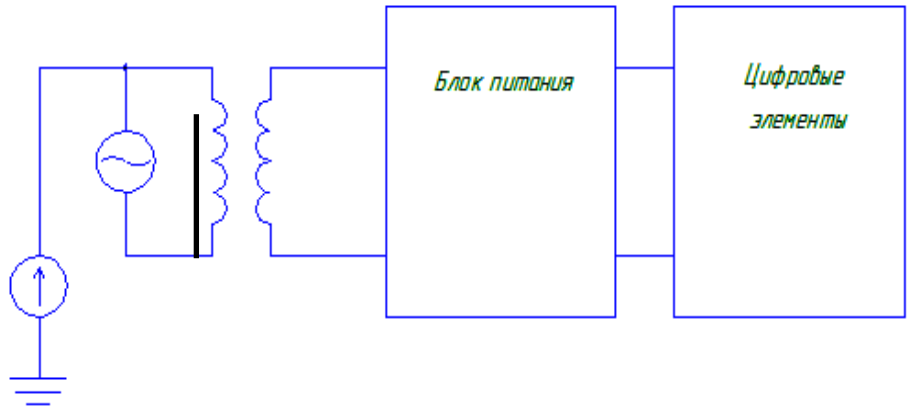

Рис. 1. Воздействие по сети питания при способе
подключения «фаза-земля»

Анализ функционирования цифровых элементов ЭС при воздействии по сети питания ЭМИ проводится в программном комплексе схемотехнического моделирования ПА-9 путем имитационного моделирования. Для проведения имитационного моделирования разработаны: модель источника преднамеренных электромагнитных воздействий по сети электропитания; упрощенная модель источника вторичного питания ЭС СКУД; модель цифрового функционального узла СКУД на основе ТТЛ логики.

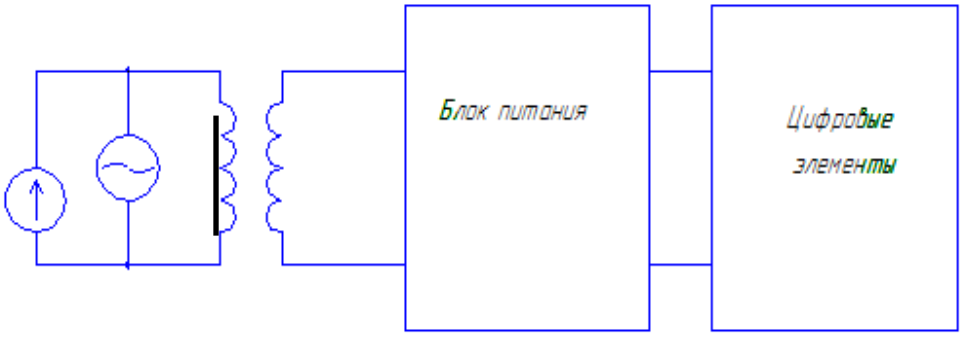

Рис. 2. Воздействие по сети питания при способе
подключения «фаза-нейтраль»

В работе рассматриваются типичные электромагнитные импульсы, воздействующие по сети питания (табл. 1). Наиболее часто, форма импульсов представляет собой двойную экспоненту.

Таблица 1. Параметры электромагнитных импульсов воздействующих по сети питания

№ импульса	Длительность фронта, $t_{фр}$	Длительность импульса на уровне 50 %, $t_{50\%}$	Пиковое значение Um, кВ	Частота повторения импульсов
1	30 нс	1 мкс-5 мкс	1,5	5 Гц
2	1 мкс	10 мкс	5-15	-
3	1,2 мкс	50 мкс	0,5-4,5	12 импульсов в минуту
4	10 мкс	700 мкс	0,5-4,5	-

В результате проведенного анализа функционирования цифровых элементов ЭС, построены графики зависимости минимальной амплитуды напряжения импульса, приводящего к сбою от его длительности воздействия при различных способах подключения генератора ЭМИ к сети электропитания (рис. 3, рис. 4).

Таким образом, по результатам проведенной работы можно сделать следующие выводы: увеличение длительности воздействия микросекундных ЭМИ в сети электропитания приводит к снижению минимального уровня амплитуды напряжения, приводящего к сбою в работе цифрового элемента; минимальный уровень амплитуды напряжения микросекундных ЭМИ в сети электропитания, приводящий к сбою цифрового элемента составляет от 500 до 7000 В; способ подключения генератора ЭМИ к сети электропитания «фаза-нейтраль» более опасна, чем «фаза-земля», с точки зрения возможного нарушения функционирования цифрового элемента. Для повышения информационной безопасности электронных систем возможно применение существующих и новых технических решений [10, 11, 12, 13].

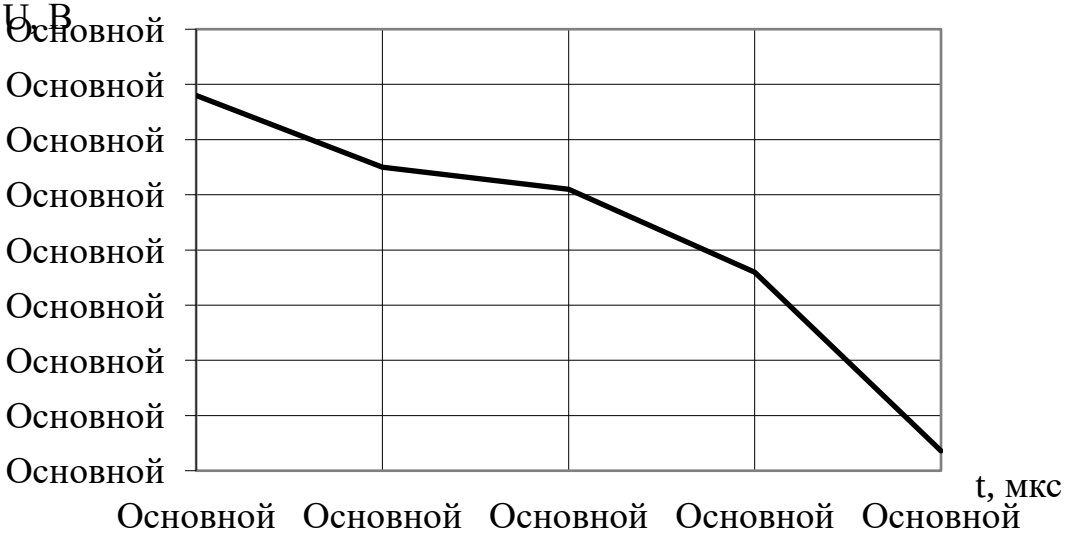

Рис. 4. Зависимость минимальной амплитуды напряжения ЭМИ, приводящего к сбою цифрового элемента от его длительности (50%) воздействия при способе подключения «фаза-земля»

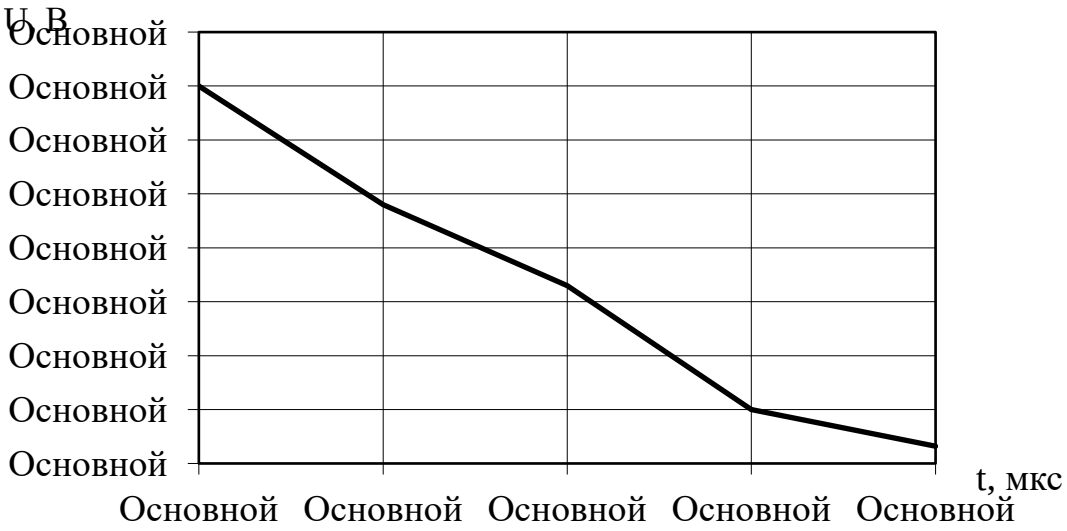

Рис. 3. Зависимость минимальной амплитуды напряжения ЭМИ, приводящего его к сбою цифрового элемента от его длительности (50%) воздействия при способе подключения «фаза-нейтраль»

Литература

1. Электромагнитный терроризм на рубеже тысячелетия // Под. ред. Т.Р. Газизова. Томск: Изд-во ТГУ, 2002. – 206 с.

2. Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникации: - М.: Издательский Дом «Технологии», 2005. – 320 с.

3. Гизатуллин З.М., Гизатуллин Р.М. Анализ качество электроэнергии в однофазной сети электропитания 220 Вольт 50 Герц // Известия высших учебных заведений. Проблемы энергетики. – 2012. – №7-8. – С. 63-71.

4. Гизатуллин З.М., Гизатуллин Р.М., Зиатдинов И.Н., Шарафутдинов И.И. Помехоустойчивость средств вычислительной техники при динамических изменениях напряжения сети электропитания // Известия высших учебных заведений. Проблемы энергетики. – 2013. – №1-2. – С. 105–115.

5. Гизатуллин З.М., Гизатуллин Р.М., Зиатдинов И.Н. Моделирование электромагнитного воздействия на электронные средства по сети электропитания здания // Известия высших учебных заведений. Проблемы энергетики. – 2014. – №7-8. – С. 104-110.

6. Гизатуллин З.М., Гизатуллин Р.М., Зиатдинов И.Н. Анализ функционирования вычислительной техники при воздействии электромагнитных помех по сети электропитания // Известия высших учебных заведений. Проблемы энергетики. – 2015. – №7-8. – С. 98-105.

7. Гизатуллин З.М., Гизатуллин Р.М. Исследование помехоустойчивости вычислительной техники при электромагнитных воздействиях по сети электропитания // Радиотехника и электроника. – 2016. – №5. – С. 500–504.

8. Гут Р.В., Кирпичников А.П., Ляшева С.А., Шлеймович М.П. Методы ранговой фильтрации в системах видеонаблюдения//Вестник технологи-

ческого университета. 2017. Т. 20. № 17. С. 71-73.

9. Обухов А.В., Ляшева С.А., Шлеймович М.П. Методы автоматического распознавания автомобильных номеров// Вестник Чувашского университета. 2016. №3. С.201-208.

10.Гизатуллин З.М., Гизатуллин Р.М., Назметдинов Ф.Р., Набиев И.И. Повышение помехоустойчивости электронных средств при электромагнитных воздействиях по сети электропитания // Журнал радиоэлектроники: электронный журнал. – 2015. – №6.- С. 2.

11.Белоусов А.О., Газизов Т.Р., Заболоцкий А.М. Многопроводная микрополосковая линия как модальный фильтр для защиты от сверхкоротких импульсов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2015. – №3. – С. 124-128.

12. Газизов А.Т., Заболоцкий А.М., Газизов Т.Р. Разложение сверхкороткого импульса в структурах с лицевой связью // Известия высших учебных заведений. Физика. – 2017. – №3. – С. 70-75.

13. Белоусов А.О., Заболоцкий А.М., Газизов Т.Р. Экспериментальное подтверждение модельной фильтрации в многопроводной микрополосковой линии // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. – №3. – С. 51-54.

Д. Шкирдов

МЕТОД ЛОВУШЕК ДЛЯ СОСТАВЛЕНИЯ ЧЕРНЫХ СПИСКОВ АТАКУЮЩИХ АДРЕСОВ

(Самарский университет)

Ни для кого не секрет, что в современном мире киберпреступления активно развиваются. Сетевые ловушки являются относительно новым способом борьбы с постоянно развивающимися сценариями атак. Сетевая ловушка (она же honeypot) –это система, представляющая из себя приманку для злоумышленника. Она обычно состоит из компьютера, программ и информации, которые вместе симулируют поведение реальной системы, являющейся частью сети. Сама ловушка изолирована и контролируется, и кажется содержит информацию или ресурс, представляющий ценность для злоумышленников [1]. Добросовестным пользователям нет смысла подключаться к такой системе, поэтому наблюдение за попытками получить доступ к ловушке и активностью в ней позволяет получить сведения об уровне угроз реальной системе. Информация, полученная в результате работы ловушки сетевых служб, систематизируется и анализируется.

Для обнаружения и анализа аномальной сетевой активности IP адресов была создана инфраструктура, основанная на понятии ловушки(приманки). В качестве ловушки используется сервер с установленным на нём программным