УДК 004.056 Вестник УрФО № 2(44) / 2022, с. 5–11

**Хижников Д. И., Михайлова У.В., Баранкова И.И.**

DOI: 10.14529/secur220201

# РАЗРАБОТКА ОБУЧАЮЩЕГО КОМПЛЕКСА ДЛЯ РАСЧЕТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

*В настоящее время защита выделенных помещений как никогда актуальна. Для оценки полноты и актуальности применяемых средств защиты, а также для анализа эффективности их применения используется специальные методические документы, разработанные ФСТЭК России.*

*В статье рассматривается обучающий тренажер для расчета побочных электромагнитных излучений. Данный тренажер имитирует реальное оборудование, предназначенного для обучения студентов ВУЗов методике проведения специсследования.*

***Ключевые слова:*** *информационные технологии, образование, виртуальные тренажеры, информационная безопасность.*

**Khizhnikov D. I., Mikhailova U.V., Barankova I.I**

# DEVELOPMENT OF A TRAINING COMPLEX FOR CALCULATING INCIDENTAL ELECTROMAGNETIC EMISSIONS

*At present, protection of allocated premises is more relevant than ever. To assess the completeness and relevance of the protection means used, as well as to analyze the effectiveness of their use, special methodological documents developed by FSTEC of Russia.*

*This article describes a training simulator for calculating incident electromagnetic emissions. This simulator simulates real equipment designed to teach students of higher education institutions the methods of special investigation*

***Keywords:*** *information technology, education, virtual trainers, information security.*

В настоящий момент технические средства (ТС), представляют большую ценность, поскольку могут обрабатывать большое количество информации за малый промежуток времени. Однако при обработке информации ТС возникает побочное электромагнитное излучение (ПЭМИ), перехватив которое злоумышленник получает доступ к обрабатываемой информации. Частотный диапазон ПЭМИ, сопровождающих информативный сигнал, простирается от единицы кГц до ГГц. В связи с этим у организации возникает потребность в защите информации и соответственно в устранении данного технического канала утечки информации.

Главное направление защиты информации от утечки за счет ПЭМИ - уменьшение отношения информативного сигнала к помехе до предела, определяемого «Нормами эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИ». Нормы определяют числовой коэффициент, при котором восстановить исходные данные невозможно. Решение этой задачи достигается снижением уровня излучений информационных сигналов, или увеличением уровня помех в частотных диапазонах.

Согласно ГОСТ Р 50922-2006 [1], специальные исследования (СИ) – комплекс мероприятий с использованием контрольно-измерительной аппаратуры, направленных на выявление и измерение информативных сигналов в каналах возможной утечки за счет побочных электромагнитных излучений и наводок, несущие скрываемую или защищаемую информацию, а также оценка защищенности информации требованиям нормативных документов по защите информации.

Для определения защищённости, исследуемой ТС в условиях эксплуатации, измеряется затухание до границы контролируемой зоны (КЗ). С учетом полученного затухания, используя данные лабораторных исследований (специальных исследования) делается вывод о защищенности объекта информатизации, а также размер зоны R2 [2].

“Зона 2” (R2) - это расстояние между ТС и условной границей, за пределами которой не возможен эффективный прием вследствие естественного затухания сигнала на фоне помех.

СИ проводятся с использованием современной измерительной аппаратуры, сертифицированной и поверенной, в соответствии с требованиями нормативных документов ФСБ России, а также ФСТЭК России. Для проведения СИ используется дорогостоящие оборудование: анализаторы спектра (Rohde&Schwarz FSH8, АКИП-4204/TG, Protek A734) с антеннами (П6-124, П6-122, П6-121).

Не многие ВУЗы для подготовки молодых специалистов по информационной безопасности имеют возможность закупить необходимое программно-аппаратное обеспечение, из-за чего студенты могут ознакомиться с методом проведения СИ только в теории. Виртуальные тренажеры способны заменить дорогостоящее оборудование и поспособствовать эффективной подготовке и развитию профессиональных навыков будущих специалистов информационной безопасности. Для решения данной проблемы разработан виртуальный тренажер позволяющий:

1. Изучить основные методики проведения СИ;

2. Освоить специальное оборудование, используемое специалистами информационной безопасности на современных предприятиях;

3. Получить навыки поиска и измерения ПЭМИ.

Разработанный виртуальный тренажер представляет собой программный комплекс, позволяющий проводить физические опыты на компьютере без непосредственного контакта с реальным оборудованием или лабораторным стендом. Он предназначен для приобретения первичных навыков в эксплуатации типовых программно-аппаратных комплексов поиска и измерения ПЭМИ.

Тренажер разработан в среде разработки Unity. Unity очень удобен для разработки средних и крупных проектов в 3D пространстве. Движок использует для написания скрипов язык программирования C#.

Разработанный виртуальный тренажер содержит меню библиотеки с информацией об оборудовании. В этом меню студент имеет возможность ознакомиться с основными характеристиками оборудования, его общим видом и габаритами. В плане дальнейшего развития тренажера предусмотрено расширение библиотеки (добавление нового оборудования, нормативные и технические документы и т.п.). На текущий момент разработана модель анализатора спектра Rohde & Schwarz FSH8 (модель 28) (рис.1), которая имеет абсолютно те же параметры и интерфейс, что и у реального образца.

Тренажер позволит обучающимся изучить возможности специализированного обо-


а б

Рис. 1. Анализатора спектра Rohde & Schwarz FSH8, где а - реальный, б - модель в тренажере

рудования, произвести СИ с использованием специальных методик, а также осуществить поиск сигнала и проанализировать его.

В качестве исследуемого объекта используется модель монитора. На экране можно задать разрешение и частоту кадров, из этих показателей будет рассчитываться частота излучения для дальнейшего нахождения этого сигнала на анализаторе спектра. Так же на экране можно задать центральную частоту.

Тренажер с правами доступа студент предусматривает два режима работы:

• В первом режиме (easy) студент знакомится с методом проведения СИ, для этого в тренажере предусмотрена система подсказок, которая будет направлять каждое действие учащегося.

• Во втором режиме (hard) студенту будет необходимо самостоятельно провести СИ, опираясь на знания полученные в ходе прохождения режима easy.

В тренажере предусмотрены различные права доступа:

• администратор (преподаватель) который может:

1. возможность изменения планировки;

2. изменения параметра исследуемых объектов (мощности сигнала выходе, μВт);

3. задавать настройки для уровня hard.

• пользователь (студент) который может:

1. изменять настройки исследуемого объекта (разрешение и частоту обновления экрана);

2. возможность изменения расположения антенны;

3. изменять свойства стен (кирпичная кладка, дерево, полистирол, бетон, пенополистирол).

Место установки исследуемого объекта не статично, как преподаватель, так и студент имеют возможность перемещения исследуемых объектов в пространстве спроектированного помещения.

Перед началом измерений студенту необходимо установить антенну измерителя напряженности поля на расстоянии R0 от исследуемого ОТСС. После этого необходимо произвести настройку ОТСС.

На ОТСС эмулируется работы Windows 7 в которой установлено два ПО:

Программа “Тест сигнал” эмитирует работу монитора и излучаемый им ПЭМИ сигнал, когда пользователь нажимает первую кнопку то на экране запускается тестовый сигнал, который генерирует частоты работы ОТСС с уровнем мощности сигнала.

После полученный данных на выявленных частотах необходима измерить уровень шума при выключенном ОТСС. Для этого нужно нажать вторую кнопку для запуска измерителя шумов.

После получения всех необходимых данных студенту становится доступна панели расчетов, в которой студенту необходимо рассчитать R2.

“Настройка” данное ПО эмитирует про-

граммно-аппаратный комплекс "Зонд-3" для воспроизведения стабильного по частоте и мощности сигнала. Для этого пользователю представлена два поля для ввода.

Анализатор не может автоматически определить частоту, на которой монитор излучает сигнал, поэтому изначально на экране анализатора спектра изображен спектр шума (рис.2). Настройка анализатора спектра пошагово и подробно показывается пользователю в виде всплывающих окон (только в режиме easy), которые меняются после успешно проведенного действия.

Если все значения посчитаны правильно на экране анализатора появится спектр сигнал + шум. На рис. 3 показана спектрограмма сигнала + шум, найденная на частоте 29 МГц мощностью 85 dBμV, который рассчитывается по формуле $dB\mu V=20Log_{10}(V_{вых}/1мкВ)$, где $V_{вых}$ – выходное напряжение, dBμV(дБмкВ) – абсолютное напряжение в децибелах относительно 1 мкВ. Полученный сигнал позволяет определить критерии защищенности.

На рис.4 показана модель помещения, в котором происходит СИ. Виртуальный тренажер учитывает реальную модель распростра-

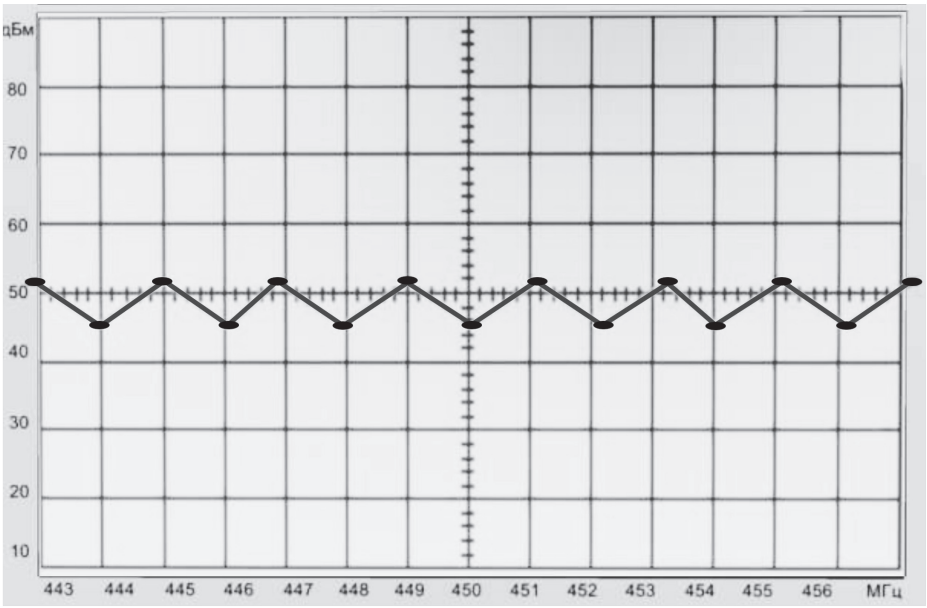


Рис. 2. Спектр шума

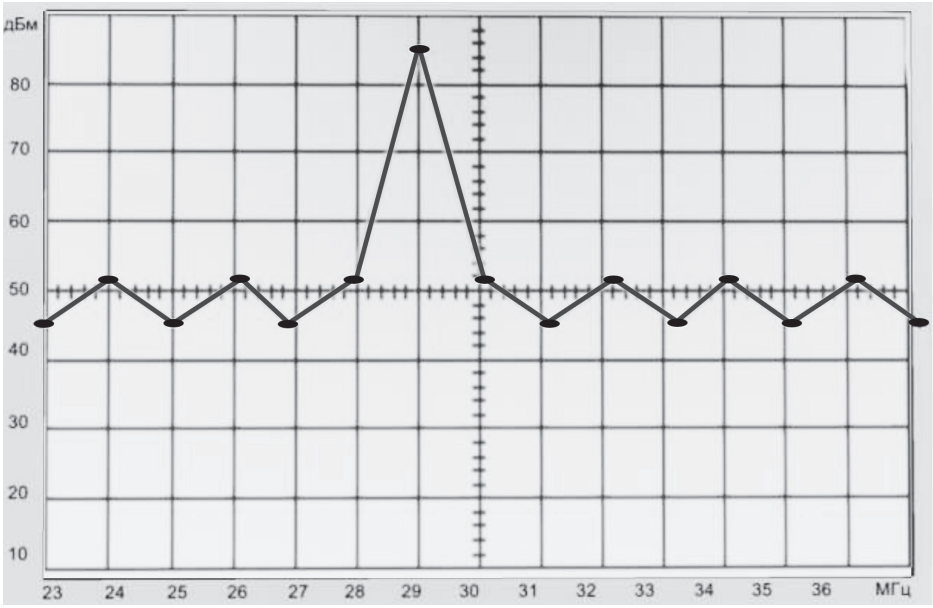


Рис. 3. Спектр сигнал+шум

нения сигнала в пространстве. Поэтому при расчетах учитываются:

1. воздушная среда;

2. заграждающие объекты без учета металлических конструкций.

В связи с политической напряженностью,

Рис. 4. Модель помещения

обострившейся вокруг России в последний год, стали особенно востребованы молодые квалифицированные специалисты в области информационной безопасности. Поэтому внедрение в образовательную программу ВУЗов виртуального тренажера обучающего комплекса для расчета ПЭМИ позволит повысить технологическую грамотность и инициативность студентов. Разработанный тренажер будет способствовать наиболее эффективному обучению по направлению информационная безопасность в части технической защиты информации, а также будет полезен специальностям: «Информационная безопасность телекоммуникационных систем» (10.05.02), «Информационная безопасность автоматизированных систем» (10.05.03).

**Литература**

1. Национальный стандарт российской федерации. ГОСТ Р 50922-2006 «ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ» [Текст], Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст. - 2021. - 4 стр.

2. Хорев А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники// Специальная техника. 2010. № 2. С. 2–15.

3. [Электронный ресурс] – Режим доступа: https://searchinform.ru/analitika-v-oblasti-ib/utechki

informatsii/sluchai-utechki-informatsii/utechka-informatsii-po-kanalam-pemin/razrabotka-meropriyatij-po-zaschite-informatsii-ot-utechki-po-kanalam-pemin/ (Дата обращения: 20.03.2022).

4. Технические Средства и Методы Защиты Информации / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. - Москва: Машиностроение, 2009. – 45 с.

5. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии / Международная конференция «Наука. Исследования. Практика». – 2019. – с. 341–345.

6. Рагозин Ю.Н. Инженерно-Техническая Защита Информации: Учебное Пособие по Физическим Основам Образования Технических Каналов Утечки Информации и по Практикуму Оценки их Опасности/ Рагозин Ю.Н. - Электрон. Текстовые Данные -СПб.: Интермедия, 2018 – 168 с.– Режим доступа: https://books.google.ru/books?id=GJOqBb3vtNUC&printsec =copyright&hl=ru#v=onepage&q&f=false

7. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Техническая защита информации / Международная конференция «Наука. Исследования. Практика». – 2017. – с. 7-10.

8. Баранкова И.И., Михайлова У.В., Романько. Е.А., Борисов В.О. Имитационный тренажер для изучения устройства и принципа работы теодолита / Магнитогорск 2011.

9. Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для оценки уровня сформированности компетенций специалиста по информационной безопасности / Информационной противодействие угрозам терроризма. 2015. Т. 2. №25. С. 26–30.

10. Имитационный тренажер для изучения устройства и принципа разработки подземных горнодобывающих систем / Имитационный тренажер. Магнитогорск 2011.

11. Михайлова У.В., Аименева А.А., Полехина А.В. Технические средства защиты информации / Актуальные проблемы современной науки. Безопасность в информационной сфере. 2012. С. 27–30

## References

1. Natsional'nyy standart rossiyskoy federatsii. GOST R 50922-2006 «OSNOVNYYe TERMINY I OPREDELENIYA» [Tekst], Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 27 dekabrya 2006 g. N 373-st. - 2021. - 4 str.

2. Khorev A. A. Tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy sredstvami vychislitel'noy tekhniki// Spetsial'naya tekhnika. 2010. № 2. S. 2–15.

3. [Elektronnyy resurs] – Rezhim dostupa: https://searchinform.ru/analitika-v-oblasti-ib/utechki informatsii/sluchai-utechki-informatsii/utechka-informatsii-po-kanalam-pemin/razrabotka-meropriyatij-po-zaschite-informatsii-ot-utechki-po-kanalam-pemin/ (Data obrashcheniya: 20.03.2022).

4. Tekhnicheskiye Sredstva i Metody Zashchity Informatsii / A.P. Zaytsev, A.A. Shelupanov, R.V. Meshcheryakov i dr. - Moskva: Mashinostroyeniye, 2009. – 45 s. 5. Mikhaylova U.V., Bykova T.V. Audit informatsionnoy bezopasnosti na predpriyatii / Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2019. – s. 341–345.

6. Ragozin YU.N. Inzhenerno-Tekhnicheskaya Zashchita Informatsii: Uchebnoye Posobiye po Fizicheskim Osnovam Obrazovaniya Tekhnicheskikh Kanalov Utechki Informatsii i po Praktikumu Otsenki ikh Opasnosti/ Ragozin YU.N. - Elektron. Tekstovyye Dannyye -SPb.: Intermediya, 2018 – 168 c.– Rezhim dostupa: https://books.google.ru/books?id=GJOqBb3vtNUC&printsec =copyright&hl=ru#v=onepage&q&f =false

7. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Tekhnicheskaya zashchita informatsii / Mezhdunarodnaya konferentsiya «Nauka. Issledovaniya. Praktika». – 2017. – s. 7-10.

8. Barankova I.I., Mikhaylova U.V., Roman'ko. Ye.A., Borisov V.O. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa raboty teodolita / Magnitogorsk 2011. 9. Barankova I.I., Mikhaylova U.V. Osobennosti formirovaniya otsenochnykh sredstv dlya otsenki urovnya sformirovannosti kompetentsiy spetsialista po informatsionnoy bezopasnosti / Informatsionnoy protivodeystviye ugrozam terrorizma. 2015. T. 2. №25. S. 26–30.

10. Imitatsionnyy trenazher dlya izucheniya ustroystva i printsipa razrabotki podzemnykh gornodobyvayushchikh sistem / Imitatsionnyy trenazher. Magnitogorsk 2011.

11. Mikhaylova U.V., Aimeneva A.A., Polekhina A.V. Tekhnicheskiye sredstva zashchity informatsii / Aktual'nyye problemy sovremennoy nauki. Bezopasnost' v informatsionnoy sfere. 2012. S. 27–30.

---

**БАРАНКОВА Инна Ильинична,** доктор технических наук, заведующая кафедрой Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: inna_barankova@mail.ru

**ХИЖНИКОВ Дмитрий Игоревич,** студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: strelok454@list.ru

**МИХАЙЛОВА Ульяна Владимировна,** кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: ylianapost@gmail.com

**BARANKOVA Inna Ilyinichna,** Doctor of Technical Sciences, Head of the Department of Informatics and Information Security f Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: inna_barankova@mail.ru

**KHIZHNIKOV Dmitry Igorevich,** student of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: strelok454@list.ru

**MIKHAILOVA Uliana Vladimirovna,** Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000. E-mail: ylianapost@gmail.com