УДК 004.058 Вестник УрФО № 2(44) / 2022, с. 43–48

Костюченко К.Л., Хабаров И.А.

DOI: 10.14529/secur220206

РАЗРАБОТКА ОБУЧАЮЩЕЙ ПРОГРАММЫ – ВИРТУАЛЬНОГО ТРЕНАЖЕРА «ПОИСК ЗАКЛАДОЧНЫХ УСТРОЙСТВ»

Статья посвящена разработке компьютерной программы, предназначенной для обучения поиску скрытых закладочных устройств – специальных технических средств, предназначенных для негласного получения информации. Показана актуальность повышения профессиональной подготовленности в вопросах технической защиты информации, особенно в условиях различных ограничений. Описана структура программы – виртуального тренажера, а также различные сценарии работы с ней. Рассмотрены основные возможности, режимы и уровни сложности разрабатываемой программы. Представлены особенности, преимущества и перспективы применения программы.

Ключевые слова: *закладочные устройства, специальные технические средства негласного получения информации, утечка информации, техническая защита информации, поисковая техника, поисковые мероприятия, обучающая программа.*

Kostyuchenko K.L., Khabarov I.A.

CREATION OF A TRAINING PROGRAM – VIRTUAL TRAINER «SEARCH FOR EAVESDROPPING DEVICE»

The article is devoted to the development of a computer program designed to teach the search for hidden eavesdropping devices – special technical means designed to secretly obtain information. The relevance of improving professional preparedness in matters of technical protection of information, especially in conditions of various restrictions, is shown. The structure of the virtual simulator program is described, as well as various scenarios for working with it. The main features, modes and levels of complexity of the developed program are considered. The features, advantages and prospects of the application of the program are presented.

Keywords: *eavesdropping devices, special technical means of secretly obtaining information, information leakage, technical protection of information, search equipment, search activities, training program.*

Вопросы защиты информации актуальны всегда. Каждый год из-за различного рода утечек информации, а также из-за незаконного доступа к носителям и средствам обработки информации у предприятий, компаний и фирм возникают множественные проблемы: материальные, финансовые, организационные, репутационные, политические.

Даже утеря (например, уход к конкуренту) 5 % всего объема конфиденциальных данных компании приводит к серьезным последствиям. Эксперты отмечают, что такого количества достаточно для утраты лидирующих позиций на рынке [1].

Примерно такая же оценка существует в отношении закладочных устройств (радиопередатчики, радиомикрофоны, диктофоны), подключаемых к телефонной линии офиса: «полгода прослушивания достаточно для того, чтобы обанкротить фирму-конкурента». Причем подобные утверждения справедливы и в век «тотальной цифровизации».

Поскольку арсенал специальных технических средств для негласного получения информации достаточно широк, а спрятаны и закамуфлированы они могут самыми неожиданными способы и в любое время, проблема борьбы с закладочными устройствами является постоянной [2–5].

Решить данную проблему позволит повышение качества обучения специалистов по защите информации, а также сотрудников смежных сфер (безопасности, охраны, управления). Для этого необходимо расширять объем знаний по технической защите информации и практических навыков по поиску закладочных устройств и каналов утечки информации.

Традиционные методы обучения, не всегда соответствуют современным требованиям. Как правило, акценты расставляются на теоретической части изучаемого материала, а для практической составляющей остается недостаточно времени. Кроме того, чисто лекционная («сухая») подача материала приводит к его неполноценному усвоению и даже к потере интереса у обучаемых. Также есть множество примеров, когда существующая учебная материальная база не позволяет рассмотреть и проанализировать весь спектр ситуаций, возникающих в реальности. Это становится особенно очевидно в нынешних условиях эпидемиологических ограничений.

В данном случае в качестве современной эффективного метода обучения можно использовать игровой метод, реализуемый в виде обучающей компьютерной программы. Суть такой обучающей программы заключается в получении обучающей среды по тематике поиска и идентификации скрытых закладочных устройств (ЗУ) – специальных технических средств для негласного получения информации.

Разрабатываемая программа «Поиск закладочных устройств» – по сути, виртуальный тренажер – позволит изучить основы поиска ЗУ и технических каналов утечки информации (ТКУИ); освоить методику проведения поисковых мероприятий; рассмотреть особенности применения всего арсенала приемов и средств поиска в различных ситуациях.

Структура программы включает в себя несколько блоков (режимов): «Теория», «Закладка ЗУ», «Поиск ЗУ» и «Поиск ТКУИ» (рис. 1).

Режим «Теория» содержит информацию по видам, конструкциям, характеристикам и вариантам установки ЗУ; по физическим основам появления ТКУИ; по теоретическим основам защиты информации; по принципам, способам и алгоритмам поисковых мероприятий; по локации нелинейностей, нелинейным локаторам (НЛ); по поисковой технике [2–5]. Завершением этого режима является тест по изученному теоретическому материалу. Успешное прохождение теста может давать право перехода к остальным режимам.

Режим «Закладка ЗУ» реализует принцип «для создания средств защиты необходимо знать средства нападения». В этом режиме обучающемуся дается возможность побыть в роли виртуального злоумышленника, который может прятать ЗУ в различных помещениях. Предполагается несколько уровней сложности, в которых варьируется конфигурация и назначение помещений, количество и характеристики ЗУ, способы и качество установки ЗУ, а также время, отводимое на установку ЗУ. Возможно создание различных условий: выбор и размещение ЗУ другим обучающимся или самой компьютерной программой (случайным образом из пополняемой библиотеки элементов); имитация окружающих помех; ограничение времени на поиск; включение встроенных контекстных подсказок и др.

Режим «Поиск ЗУ» (антипод режима «Закладка ЗУ») предназначен для обучения нахождению и нейтрализации ЗУ. В этом режиме предусматривается выбор нелинейного локатора (по тактико-техническим характе-

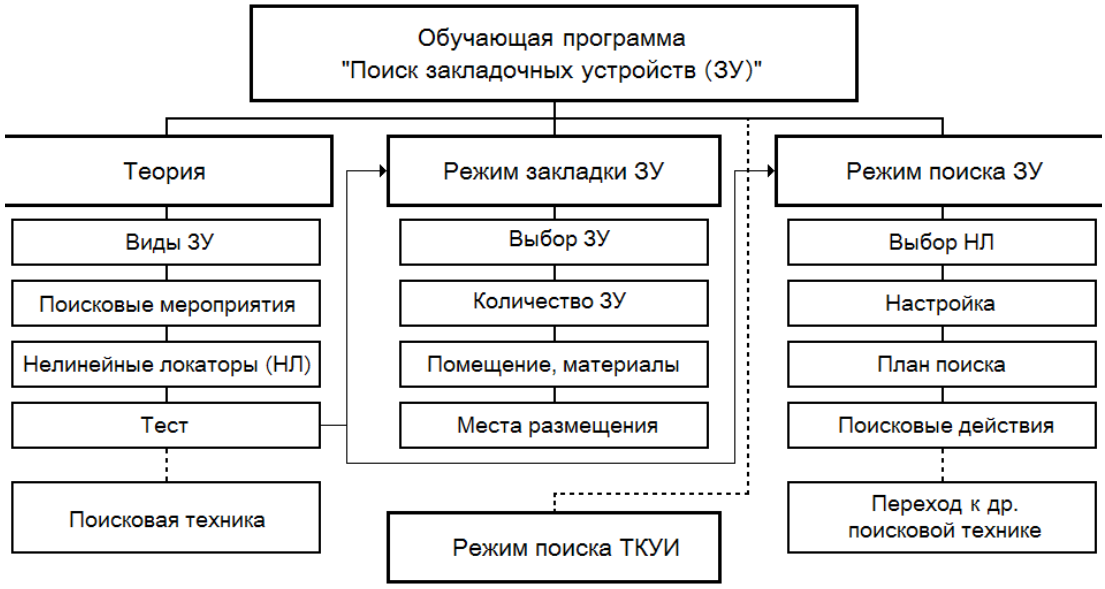

Рис. 1. Структура обучающей программы

ристикам); настройка (калибровка поисковой аппаратуры); выбор иной поисковой техники из имеющегося арсенала. Всё это можно сделать на нескольких уровнях сложности, определяемыми параметрами помещений, способами установки ЗУ, их количеством и др.

Режим «Поиск ТКУИ» включает в себя блоки программы, связанные с поиском и ликвидацией технических каналов утечки информации. Данный режим из-за достаточно большого объема предполагается реализовывать на завершающих этапах.

Основой для создания программы является межплатформенная среда разработки компьютерных игр – платформа разработки 3D-контента реального времени Unity [6]. Крупными разработчиками и независимыми студиями на «платформе Unity» написано большое множество программ: игр, приложений и визуализаций математических моделей. Выбранная среда обладает рядом имеющихся преимуществ: возможность визуализации процесса разработки, межплатформенная поддержки, модульная система компонентов и т.п. Указанные особенности отличают представляемую разработку от уже существующих аналогичных виртуальных тренажеров, например [7].

В данный момент программа находится на этапе активной разработки: вырабатывается стиль и дизайн программы (скриншоты на рис. 2–5), определяется соотношение между элементами двухмерной и трёхмерной графики, апробируются варианты представления помещений, отрабатывается перевод приемов работы с поисковой техникой (прежде всего, нелинейным локатором) в цифровую форму, пополняется теоретический раздел и база характеристик используемых устройств, создается генератор уровней (сценариев) сложности.

На рис. 2 представлено основное меню выбора режима. Ознакомление с техническими характеристиками поисковой аппаратуры в режиме «Теория» иллюстрируется на примере нелинейного локатора «Лорнет» (рис. 3). В загрузочном меню выбранного уровня сложности в режиме «Поиск» (рис. 4) выдается поисковая задача с кратким ее описанием и схемой помещения. На рис. 5 изображен скриншот панели управления нелинейным локатором «ORION» во время поиска ЗУ в помещении учебного класса.

Заключение

Использование в учебном процессе предлагаемой обучающей программы «Поиск закладочных устройств» позволит:

– усилить интерес обучающихся к тематике отдельных направлений информационной безопасности;

– за счет теоретической составляющей программы расширить кругозор обучающихся и базу их знаний в сфере технический защиты информации;

– иметь возможность изучать учебный материал по обнаружению каналов утечки информации как в очном, так и в дистанционном варианте (например, в условиях сложной эпидемиологической обстановки);

Рис. 2. Скриншот меню выбора режима

Рис. 3. Скриншот страницы в режиме «Теория»

Рис. 4. Загрузочное меню режима «Поиск»

Рис. 5. Скриншот работы с нелинейным локатором (с индикацией уровней мощности передачи и принятых сигналов 2-й и 3-й гармоник)

– благодаря игровому методу набрать определенный опыт проведения поисковых мероприятий за счет рассмотрения («проигрывания» в виртуальном пространстве) большого количества самых разнообразных ситуаций, в т.ч. с учетом появления новой техники;

– снизить определенным образом затраты на процесс обучения;

– повысить общую эффективность подготовки и тренажа специалистов в сере защиты информации;

– приобрести необходимые компетенции по тематике технической защиты информации специалисты смежных специальностей (IT, связь, безопасность, охрана и др.).

Литература

1. ПАО «Ростелеком-Солар». Финансовые и репутационные потери от утечек информации [Электронный ресурс] режим доступа: https://rt-solar.ru/products/solar_dozor/blog/2163/ (дата обращения: 12.01.2022).

2. Защита информации: устройства несанкционированного съема информации и борьба с ними: Учебно-практическое пособие. / С.Н. Козлов – М.: Академический проспект, 2018.

3. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов – М.: Горячая линия – Телеком, 2018.

4. Выявление специальных технических средств несанкционированного получения информации / Г.А. Бузов – М.: Горячая линия – Телеком, 2019.

5. Технические средства и методы защиты информации. Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева и А.А. Шелупанова – М.: Горячая линия – Телеком, 2020.

6. Платформа Unity. [Электронный ресурс] режим доступа: https://unity.com/ru/products/unity-platform (дата обращения: 05.11.2021).

7. Шпак В.А., Кремлев Е.С., Михайлова У.В. Разработка виртуального тренажера для оценки защищенности акустической информации в контролируемом помещении / Вестник УрФО. Безопасность в информационной сфере. № 2(36) / 2020, с. 10–16.

References

1. PAO «Rostelekom-Solar». Finansovye i reputacionnye poteri ot utechek informacii [Financial and Reputational Losses from Information Leaks]. Available at: https://rt-solar.ru/products/solar_dozor/blog/2163/ (accessed 12 January 2022).

2. Kozlov S.N. Zashhita informacii: ustrojstva nesankcionirovannogo s'ema informacii i bor'ba s nimi:

Uchebno-prakticheskoe posobie. [Information Protection: Devices for Unauthorized Removal of Information and Combating Them: An Educational and Practical Guide]. Moscow, Akademicheskij prospekt, 2018.

3. Buzov G.A. Zashhita informacii ogranichennogo dostupa ot utechki po tehnicheskim kanalam /– [Protection of Restricted Access Information from Leakage Through Technical Channels]. Moscow, Gorjachaja linija – Telekom, 2018.

4. Buzov G.A. Vyjavlenie special'nyh tehnicheskih sredstv nesankcionirovannogo poluchenija informacii [Finding Special Technical Means of Unauthorized Receipt of Information]. Moscow, Gorjachaja linija – Telekom, 2019.

5. Zajcev A.P., Shelupanov A.A., Meshherjakov R.V. Tehnicheskie sredstva i metody zashhity informacii. Uchebnik dlja vuzov / [Technical Means and Methods of Information Protection. Textbook for Universities]. Moscow, Gorjachaja linija – Telekom, 2020.

6. Platforma Unity. [Platform Unity]. Available at: https://unity.com/ru/products/unity-platform (accessed 5 May 2021).

7. Shpak V.A., Kremlev E.S., Mihajlova U.V. Razrabotka virtual'nogo trenazhera dlja ocenki zashhishhennosti akusticheskoj informacii v kontroliruemom pomeshhenii [Development of a Virtual Trainer for Assessing the Protection of Acoustic Information in a Controlled Room]. Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. № 2(36) / 2020, p. 10–16.

КОСТЮЧЕНКО Константин Леонидович, кандидат технических наук, доцент, доцент кафедры Информационных технологий и защиты информации, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: KKostyuchenko@usurt.ru.

ХАБАРОВ Игорь Андреевич, студент, Уральский государственный университет путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: WonderChief@mail.ru.

KOSTYUCHENKO Konstantin Leonidovich, Candidate of Engineering Sciences, Docent, Associate Professor of the Department of Information Technology and Information Security, Ural State University of Railway Transport. 66 Kolmogorov str., Yekaterinburg, 620034. E-mail: KKostyuchenko@usurt.ru.

KHABAROV Igor Andreevich, Student, Ural State University of Railway Transport. 66 Kolmogorov str., Yekaterinburg, 620034. E-mail: WonderChief@mail.ru.