УДК 621.396 DOI 10.23683/2311-3103-2018-2-247-256

В.В. Василенко, С.В. Рыженко

МЕТОДИЧЕСКИЙ ПОДХОД К ВЫБОРУ СПОСОБА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЁТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И АТТЕСТАЦИИ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Задачей статьи является проведение анализа существующих типов средств защиты информации от утечки за счёт побочных электромагнитных излучений, методов их практического (наиболее распространённого) применения на современных объектах информатизации (объектах вычислительной техники), введение и критериальное определение понятия распределённого объекта информатизации. Целью статьи является рассмотрение различных вариантов построения систем защиты информации от утечки за счёт побочных электромагнитных излучений от средств вычислительной техники. Предложен подход к решению задачи выбора способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации для требуемого состава объекта вычислительной техники на начальном этапе проектирования для установленных экспертным путем технико-экономических условий. Введённые технико-экономические показатели не только охватывают полную картину подготовки и аттестации объекта информатизации, соответствуют актуальным требованиям Федеральной службы по техническому и экспортному контролю. Сопоставление технико-экономических показателей для различных подходов создания систем защиты информации от утечки за счёт побочных электромагнитных излучений позволяет ввести показатель целесообразности и определить критерии выбора одного из подходов на начальном этапе проектирования. Практическая реализуемость доказана на рассмотренном примере, использующем значения технико-экономических показателей сформированных на основе коммерческих предложений на проведение защитных мероприятий и аттестации одного объекта информатизации на базе СВТ четырёх организаций-исполнителей, выполняющих работы по защите информации. В качестве основных выводов можно констатировать факт, что предложенный методический подход позволяет на начальном этапе проектирования для установленных экспертным путем технико-экономических условий определить целесообразность использования одного из возможных способов создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации.

Средство активной защиты; техническое средство; средство вычислительной техники; генератор шума; объект информатизации, побочные электромагнитные излучения.

V.V. Vasilenko, S.V. Ryzhenko

METHODICAL APPROACH TO CHOOSING THE WAY OF CREATION INFORMATION SECURITY SYSTEMS TO PROVIDE INFORMATION PROTECTION FROM LEAKING BY COLLATERAL ELECTROMAGNETIC RADIATION AND ATTESTATION OF THE ADP EQUIPMENT OBJECTS

The task of this article is to analyze existing types of information protection instruments which are used against leaking by collateral electromagnetic radiation, most common methods of their practical application in modern information objects (ADP computer objects), introduction and definition the concept of distributed information object. The goal of this article is also reviewing various options of constructing information security systems to provide information protection from leaking by collateral electromagnetic radiation from the ADP equipment objects. Offered is the approach to solving the problem of choosing the way of creation information security systems to provide information protection from leaking by collateral electromagnetic radiation and also the way of ADP equipment objects attestation for the required composition of protected computing equipment at the initial design stage for specific technical and economic conditions set by experts. The introduced technical and economic indicators

cover a comprehensive view of information object's preparation and attestation and meet the current requirements of the Federal service for technical and export control. Comparison of technical and economic indicators for different approaches to create information security systems that provide information protection from leaking by collateral electromagnetic radiation allows introducing an expediency indicator and determining the criteria for choosing one of the approaches at the initial design stage. The practical feasibility is proved by the example with technical and economic indicators formed on commercial offers for carrying out protective measures and attestation at one information object by four organizations performing information protection. As main conclusions, we state the fact that proposed methodical approach at initial design stage allows determining the feasibility of using one of the possible ways to create an information security system that provide information protection from leaking by collateral electromagnetic radiation and information objects attestation for specific technical and economic conditions set by experts.

Means of the active protection; technical tool; means of an ADP equipment; noise generator; object of informatization; collateral electromagnetic radiations.

1. Введение. В настоящее время тенденция развития средств вычислительной техники (СВТ), направленная на повышение их производительности, ведёт к увеличению энергопотребления основных компонентов и узлов, таких как графический процессор, оперативная память, контроллеры различных интерфейсов и т.п., что в свою очередь повышает уровень побочных электромагнитных излучений (ПЭМИ) от СВТ [1]. Использование для обработки защищаемой информации СВТ более раннего поколения становится невозможным ввиду отсутствия их производства и поддержки.

Таким образом, для современных защищаемых СВТ актуальной становится задача обеспечения не только норм электромагнитной совместимости [2], но и норм защиты информации от утечки за счёт ПЭМИ [3] при больших значениях радиусов зон их распространения. Данное обстоятельство приводит к необходимости использования средств активной защиты (САЗ) информации от утечки за счёт ПЭМИ на объектах вычислительной техники (ОВТ), на которых защищённость информации не обеспечивается пространственным разносом СВТ относительно мест возможного перехвата сигналов ПЭМИ [3–6].

В сложившейся практике выбор САЗ от утечки за счёт ПЭМИ на объектах вычислительной техники сводится к применению отдельных генераторов электромагнитного шума (ГШ) или их совокупностей (систем) [7]. Наиболее распространенными методами, применяемыми для активной защиты информации от утечки за счёт ПЭМИ, являются методы совмещённого и распределённого размещения ГШ [8].

2. Существующие подходы к построению систем защиты информации от утечки за счёт ПЭМИ. При совмещённом использовании генераторы шума устанавливаются в непосредственной близости относительно средств вычислительной техники, предназначенных для обработки защищаемой информации (ЗСВТ), порой такие генераторы шума называют автономными маскираторами [9].

Такой подход к применению средств активной защиты, при всей его очевидной функциональной эффективности, имеет существенный недостаток, заключающийся в избыточности средств защиты и, как следствие, дороговизне реализации защиты при значительном количестве средств вычислительной техники.

При распределённом методе размещения генераторов шума относительно средств вычислительной техники на практике применяется два типа средств активной защиты информации:

- точечные (ГШ обладает встроенной антенной или внешней антенной системой, геометрические размеры которых сопоставимы с размерами генератора шума);
- пространственные (ГШ обладает внешней антенной системой, представляющей из себя, например, рамку, изготовленную из проводника тока, имеющую значительные геометрические размеры) [10–11].

Пространственные средства активной защиты монтируются, как правило, на этапе капитального ремонта или строительства помещения (здания), в котором планируется размещение средств вычислительной техники, путём монтажа антенных систем генератора шума в ограждающие конструкции помещения (здания). Использование данного типа средств активной защиты информации, зачастую, приводит к избыточности создаваемого электромагнитного шума и редко применимо на практике.

Точечные генераторы шума устанавливаются в произвольных точках пространства и могут обеспечивать защищённость как отдельных средств вычислительной техники, так и их групп (локальных вычислительных сетей). При этом для оценки защищённости информации, обрабатываемой средствами вычислительной техники, допускается учитывать помехи, создаваемые несколькими генераторами шума.

Указанный подход наиболее актуален для распределённых объектов информатизации, включающих в себя группу средств вычислительной техники, используемых для обработки защищаемой информации.

В качестве критериев отнесения объекта информатизации к распределённому могут рассматриваться [12]:

превышение максимального расстояния между местами возможного (планируемого) размещения средств вычислительной техники над расстоянием до ближайшего места возможного размещения приёмника ПЭМИ более, чем 10%;

наличие большого количества ЗСВТ, линий обмена данными, вспомогательных технических средств и систем, сосредоточенных в одном здании или помещении в пределах охраняемой территории объекта.

3. Методический подход к выбору способа создания системы защиты информации от утечки за счёт ПЭМИ и аттестации объектов вычислительной техники. Выбор способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации возможен среди трех применяемых на сегодняшний день подходов [13-15]:

- автономный (генератор шума используется в составе объекта вычислительной техники, включающего одно ЗСВТ);
- групповой (генераторы шума используются для защиты нескольких объектов вычислительной техники, имеющих в своём составе по одному ЗСВТ);
- системный (генераторы шума объединены в пространственную систему и используются для защиты нескольких ЗСВТ, входящих в состав единого объекта вычислительной техники).

Для каждого из трех подходов представляется возможным оценивать совокупность трудозатрат по защите объектов информатизации на базе средств вычислительной техники и их аттестации: $С_{авт,}$ – при автономном подходе, $С_{гр}$ – групповом, $С_{сист}$ – системном [16].

Полученные оценки сопоставляются друг с другом путём расчёта разницы трудозатрат для рассматриваемых подходов:

$$\begin{aligned} \Delta С_{I} &= С_{авт} - С_{гр}, \\ \Delta С_{II} &= С_{авт} - С_{сист}, \\ \Delta С_{III} &= С_{гр} - С_{сист}. \end{aligned} \qquad (1)$$

Выбор экономически выгодного подхода предлагается осуществлять с учётом выполнения следующих условий:

для системного подхода

$$\begin{cases}(\Delta C_I > \Delta S)\cap(\Delta C_{II} > \Delta S)\cap(\Delta C_{III} > \Delta S),\\ (\Delta C_I \le \Delta S)\cap(\Delta C_{II} > \Delta S)\cap(\Delta C_{III} > \Delta S);\end{cases} \quad (2)$$

для группового подхода

$$\begin{cases}(\Delta C_I > \Delta S)\cap(\Delta C_{II} > \Delta S)\cap(\Delta C_{III} \le \Delta S),\\ (\Delta C_I > \Delta S)\cap(\Delta C_{II} \le \Delta S)\cap(\Delta C_{III} \le \Delta S);\end{cases} \quad (3)$$

для автономного подхода

$$\begin{cases}(\Delta C_I \le \Delta S)\cap(\Delta C_{II} \le \Delta S)\cap(\Delta C_{III} > \Delta S),\\ (\Delta C_I \le \Delta S)\cap(\Delta C_{II} \le \Delta S)\cap(\Delta C_{III} \le \Delta S),\\ (\Delta C_I > \Delta S)\cap(\Delta C_{II} \le \Delta S)\cap(\Delta C_{III} > \Delta S),\\ (\Delta C_I \le \Delta S)\cap(\Delta C_{II} > \Delta S)\cap(\Delta C_{III} \le \Delta S),\end{cases} \quad (4)$$

где $\Delta S = (\max\limits_{k\,\epsilon\,K} S_k - \min_{k\,\epsilon\,K} S_k)$ – значение максимального отклонения оценок трудозатрат при выборе организации-исполнителя специальных работ из опрошенного множества организаций K с трудозатратами S_k, включающих аттестацию объекта информатизации, состоящего из одного ЗСВТ и защищаемого одним САЗ

$$S_k = {}_k\mathrm{C}_{\text{авт}_1} = {}_k\mathrm{C}_{\text{гр}_1} = {}_k\mathrm{C}_{\text{сист}_1}, k\,\epsilon\,K; \quad (5)$$

${}_k\mathrm{C}_{\text{авт}_1}, {}_k\mathrm{C}_{\text{гр}_1}, {}_k\mathrm{C}_{\text{сист}_1}$ – стоимость проведения защитных мероприятий и аттестации объекта информатизации, состоящего из одного ЗСВТ, с применением единственного генератора шума.

Объединив условия для различных подходов (2-4), и с учётом того, что два последних компонента системы (4) являются пустым множеством Ø, критерий выбора способа защиты описывается выражением

$$\begin{bmatrix}\text{Способ}\\ \text{создания СЗИ}\end{bmatrix} \rightarrow \begin{cases}\text{СИСТЕМНЫЙ, если } (\Delta\mathrm{C}_{II} > \Delta S)\cap(\Delta\mathrm{C}_{III} > \Delta S),\\ \text{ГРУППОВОЙ, если } (\Delta\mathrm{C}_{I} > \Delta S)\cap(\Delta\mathrm{C}_{III} \le \Delta S),\\ \text{АВТОНОМНЫЙ, } (\Delta\mathrm{C}_{I} \le \Delta S)\cap(\Delta\mathrm{C}_{II} \le \Delta S),\end{cases} \quad (6)$$

Совокупность трудозатрат для различных подходов предлагается определить из технико-экономических показателей [17–19], выраженных в трудозатратах, перечень которых приведён в табл. 1.

Таблица 1

Технико-экономические показатели защиты и аттестации ОВТ

№ п/п	Наименование показателя	Условное обозначение
	Обследование объекта информатизации	C_1
	Разработка программы аттестационных испытаний объекта информатизации	C_2
	Проведение специальной проверки технических средств	C_3
	Проведение специальных исследований технических средств	C_4
	Контроль защищённости обрабатываемой информации	C_5
	Разработка системы защиты информации	C_6

№ п/п	Наименование показателя	Условное обозначение
	Закупка, поставка средств активной защиты информации	C_7
	Монтаж и настройка средств активной защиты	C_8
	Разработка инструкции по эксплуатации средств активной защиты	C_9
	Закупка, поставка средств защиты от несанкционированного доступа	C_{10}
	Закупка, поставка антивирусной программы	C_{11}
	Установка и настройка средств защиты от несанкционированного доступа	C_{12}
	Установка и настройка антивирусной программы	C_{13}
	Оценка эффективности средств активной защиты информации	C_{14}
	Проведение комплексных аттестационных испытаний объекта информатизации	C_{15}
Сумма		S

Для автономной системы защиты информации трудозатраты составляют количество защищаемых СВТ, умноженное на трудозатраты на выполнение защитных мероприятий и аттестации одного объекта информатизации. Совокупность трудозатрат, включая закупку и поставку средств защиты, рассчитывается по формуле [20]

$$C_{авт} = N_{зсвт} \cdot \sum_{n=1}^{15} C_n, \quad (7)$$

где $N_{ЗСВТ}$ – количество защищаемых СВТ.

Если использовать средства активной защиты информации от утечки за счёт побочных электромагнитных излучений для группы ЗСВТ, то трудозатраты складываются из работ по разработке единой системы защиты информации от утечки за счёт побочных электромагнитных излучений, работ по закупке и монтажу средств активной защиты для всех СВТ и работ по подготовке и аттестации каждого ОВТ. Совокупность трудозатрат рассчитывается по формуле

$$C_{гр} = C_{саз} + N_{гш} \cdot \sum_{n=7}^{8} C_n + N_{зсвт} \cdot \sum_{n=1-5;\ 9-15} C_n, \quad (8)$$

где $N_{гш}$ – количество генераторов шума (средств активной защиты), $C_{саз}$ – трудозатраты на разработку системы защиты. Естественно предположить, что затраты $C_{саз}$ для группового и автономного подходов превышают не менее чем в K_p раз затраты C_6,

$$C_{саз} = K_p C_6. \quad (9)$$

Для системного подхода трудозатраты складываются из затрат на разработку единой системы защиты, работ по закупке и монтажу средств активной защиты, работ по подготовке ОВТ к аттестации и работ по аттестации единого объекта вычислительной техники. Совокупность трудозатрат рассчитывается по формуле

$$C_{сист} = C_{саз} + N_{гш} \cdot \sum_{n=7}^{8} C_n + N_{зсвт} \cdot \sum_{n=1;3-5;\ 10-14} C_n + \sum_{n=2;9;15} C_n. \quad (10)$$

Таким образом, при построении системы защиты информации от утечки за счёт побочных электромагнитных излучений применительно к принятым технико-экономическим условиям представляется возможным на начальном этапе проектирования определить целесообразность использования способа создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации для требуемого количества защищаемых СВТ.

Предложенный методический подход позволяет определить указанную целесообразность на начальном этапе проектирования для установленных экспертным путем технико-экономических условий.

4. Пример реализации предложенного методического подхода к выбору способа создания системы защиты информации от утечки за счёт ПЭМИ и аттестации объектов вычислительной техники. В качестве примера выбора способа защиты информации от утечки за счёт побочных электромагнитных излучений и определения количества ЗСВТ рассмотрен вариант на основе коммерческих предложений на проведение защитных мероприятий и аттестации одного объекта информатизации на базе СВТ четырёх организаций-исполнителей, выполняющих работы по защите информации более 10 лет.

В табл. 2 приведены технико-экономические показатели и их значения в трудозатратах, сформированных на основе экономических нормативов (средней заработной платы в этих коммерческих организациях).

Таблица 2

Значения технико-экономических показателей защиты и аттестации ОВТ

№ п/п	Условное обозначение	Значение показателя, человек/день				
		Организация № 1	Организация № 2	Организация № 3	Организация № 4	Среднее арифметическое значение
	C_1	1,5	2,3	2,3	3,0	2,3
	C_2	3,0	2,4	0,9	3,0	2,4
	C_3	2,4	3,8	3,0	3,0	3,1
	C_4	1,8	3,2	2,6	2,6	2,6
	C_5	2,4	4,1	3,6	6,0	4,1
	C_6	1,5	2,4	1,5	4,5	2,5
	C_7	6,0	6,4	9,0	5,4	6,7
	C_8	0,6	0,7	1,8	0,4	0,9
	C_9	0,3	0,4	2,1	0,9	1,0
	C_{10}	3,6	7,0	5,4	5,3	5,4
	C_{11}	2,1	1,6	2,4	2,3	2,1
	C_{12}	1,5	1,6	2,6	3,0	2,2
	C_{13}	0,3	0,4	0,8	1,5	0,8
	C_{14}	3,0	2,9	2,7	4,5	3,3
	C_{15}	6,0	3,7	4,5	4,5	4,7
S		36,0	42,9	45,2	49,9	44,1

Для примера примем, что трудозатраты на разработку системы защиты для группового и системного подходов превышают в 25 раз затраты для автономного подхода, что подтверждено результатами опроса организаций-исполнителей ($K_p = 25$).

Проведя расчёты по средним арифметическим значениям технико-экономических показателей трёх подходов создания системы защиты информации и аттестации, получим систему выражений, определяющих зависимости трудозатрат от количества ЗСВТ и генераторов шума.

$$\begin{cases} C_{\text{авт}} = 44{,}1N_{\text{зсвт}}, \\ C_{\text{гр}} = 34{,}0N_{\text{зсвт}} + 7{,}6N_{\text{гш}} + 62{,}5, \\ C_{\text{сист}} = 25{,}9N_{\text{зсвт}} + 7{,}6N_{\text{гш}} + 70{,}6. \end{cases} \quad (11)$$

По приведённым зависимостям построены графики на рис. 1 при $N_{\text{зсвт}} = N_{\text{гш}}$.

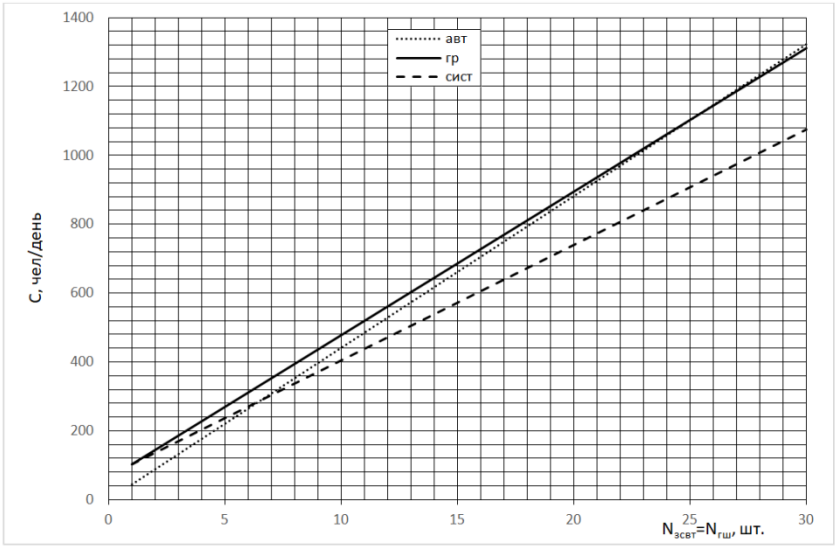

Рис. 1. Зависимость трудозатрат на создание системы защиты информации и аттестации объекта информатизации от количества ЗСВТ и ГШ

Сопоставив результаты расчётов трудозатрат в соответствии с выражениями (1) и (11), получим

$$\begin{gathered}\Delta C_I = 10{,}1N_{\text{зсвт}} - 7{,}6N_{\text{гш}} - 62{,}5,\\ \Delta C_{II} = 18{,}2N_{\text{зсвт}} - 7{,}6N_{\text{гш}} - 70{,}6,\\ \Delta C_{III} = 8{,}1N_{\text{зсвт}} - 8{,}1.\end{gathered} \tag{12}$$

Исходя из условия выбора подхода «АВТОНОМНЫЙ» из выражения (6) при $\Delta S = (49{,}9 - 36{,}0) = 13{,}9$ с учётом $N_{\text{зсвт}} = N_{\text{гш}}$ получим систему неравенств:

$$\begin{cases}10{,}1N_{\text{зсвт}} - 7{,}6N_{\text{гш}} \le 76{,}4,\\ 18{,}2N_{\text{зсвт}} - 7{,}6N_{\text{гш}} \le 84{,}5,\\ N_{\text{зсвт}} = N_{\text{гш}}.\end{cases} \tag{13}$$

Решение системы: $N_{\text{зсвт}} = N_{\text{гш}} \le 7$.

Для подхода «ГРУППОВОЙ» аналогично получим систему неравенств

$$\begin{cases}10{,}1N_{\text{зсвт}} - 7{,}6N_{\text{гш}} > 76{,}4,\\ 8{,}1N_{\text{зсвт}} \le 22{,}0,\\ N_{\text{зсвт}} \ge N_{\text{гш}}.\end{cases} \tag{14}$$

Система неравенств (14) не имеет решений, что представляется логичным, так как трудозатраты на аттестационные мероприятия при СИСТЕМНОМ подходе будут всегда меньше, чем сумма трудозатрат того же объёма АВТОНОМНОГО и ГРУППОВОГО подходов, при равенстве прочих трудозатрат. Исключение составляет случай, когда $N_{\text{зсвт}} = 1$, однако трудозатраты на проектирование системы защиты одного ЗСВТ при ГРУППОВОМ подходе превышают затраты для АВТОНОМНЫХ СВТ ($C_{\text{саз}} > C_6$) при прочих равных трудозатратах.

Для подхода «СИСТЕМНЫЙ» получим систему неравенств

$$\begin{cases}18{,}2N_{\text{зсвт}} - 7{,}6N_{\text{гш}} > 84{,}5,\\ 8{,}1N_{\text{зсвт}} > 22{,}0,\\ N_{\text{зсвт}} \ge N_{\text{гш}}.\end{cases} \tag{15}$$

С учётом решения системы неравенств (13) данная система имеет следующее решение:

$$N_{\text{зсвт}} \geq 8 \text{ при } N_{\text{гш}} \in [1; \infty]. \quad (16)$$

Таким образом, при построении системы защиты информации от утечки за счёт побочных электромагнитных излучений применительно к принятым технико-экономическим условиям для восьми и более защищаемых СВТ при условии использования отдельного ГШ для каждого ЗСВТ рационально (экономически выгодно) рассматривать их, как единый распределённый объект информатизации с системным подходом защиты.

Выводы. Предложенный методический подход позволяет на начальном этапе проектирования для установленных экспертным путем технико-экономических условий определить целесообразность использования одного из возможных способов создания системы защиты информации от утечки за счёт побочных электромагнитных излучений и аттестации объектов информатизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 21552-84. Средства вычислительной техники. Общие технические требования, приёмка, методы испытаний, маркировка, упаковка, транспортирование и хранения.
2. ГОСТ Р 51318.16.2.3-2009. Совместимость технических средств электромагнитная. Требования к аппаратуре для измерения параметров индустриальных помех и помехоустойчивости и методы измерений.
3. ГОСТ Р 53112-2008. Защита информации. Комплексы для измерения параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.
4. Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН), Гостехкомиссия России, 1998 г., в редакции 2006 г.
5. Специальные требования и рекомендации по защите информации (СТР) 1997 г.
6. ГОСТ 29339-92. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования.
7. *Парфенов В.И.* Защита информации. Словарь. – Воронеж, 2003. – 292 с.
8. Сборник методических документов ФСТЭК России, 2005.
9. *Хорев А.А.* Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Ч. 2 // Специальная техника. – 2011. – № 4.
10. Методика ПСАЗ от утечки за счёт ПЭМИН распределённого объекта информатизации.
11. Приказ ФСТЭК России от 16 мая 2014 г. № 013.
12. *Рыженко С.В., Василенко В.В.* Увеличение жизненного цикла защищённых объектов вычислительной техники за счёт построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений от основных технических средств и систем // Материалы XIV Международной научно-практической конференции «Информационная безопасность – 2015». – Таганрог, 2015.
13. *Кондратьев А.В.* Техническая защита информации. Практика работ по оценке основных каналов утечки. – М., 2016. – 304 с.
14. *Котенко В.В., Румянцев К.Е.* Теория информации и защита телекоммуникаций. – Ростов-на-Дону, 2009. – 369 с.
15. *Сухарев Е.М.* Общесистемные вопросы защиты информации. – М., 2003. – 144 с.
16. *Таха Хемди А.* Введение в исследование операций. – М., 2005. – 912 с.
17. Приказ ФСТЭК России от 20 октября 2016 г. № 025.
18. *Голяков А.А., Горбатов В.С., Дураковский А.П., Панин А.Е., Чистяков М.С.* Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации. – М., 2014. – 208 с.
19. *Сухарев Е.М.* Модели развития технических разведок и угроз безопасности информации. – М., 2003. – 296 с.
20. *Выгодский М.Я.* Справочник по высшей математике. – М.: Наука, 1966.

REFERENCES

1. GOST 21552-84. Sredstva vychislitel'noy tekhniki. Obshchie tekhnicheskie trebovaniya, priemka, metody ispytaniy, markirovka, upakovka, transportirovanie i khraneniya [Computer aids. General technical requirements, acceptance, test methods, marking, packaging, transportation and storage].
2. GOST R 51318.16.2.3-2009. Sovmestimost' tekhnicheskikh sredstv elektromagnitnaya. Trebovaniya k apparature dlya izmereniya parametrov industrial'nykh pomekh i pomekhoustoychivosti i metody izmereniy [Compatibility of technical means electromagnetic. Requirements for the equipment for measuring the parameters of industrial noise and noise immunity and measurement methods].
3. GOST R 53112-2008. Zashchita informatsii. Kompleksy dlya izmereniya parametrov pobochnykh elektromagnitnykh izlucheniy i navodok. Tekhnicheskie trebovaniya i metody ispytaniy [Information protection. Complexes for measuring parameters of side electromagnetic radiation and crosstalk. Technical requirements and test methods].
4. Sbornik norm zashchity informatsii ot utechki za schet pobochnykh elektromagnitnykh izlucheniy i navodok (PEMIN), Gostekhkomissiya Rossii, 1998 g., v redaktsii 2006 g. [Collection of standards of information protection from leakage due to side electromagnetic radiation and interference (pemin), Gostekhkomissiya of Russia, 1998, as amended in 2006].
5. Spetsial'nye trebovaniya i rekomendatsii po zashchite informatsii (STR) 1997 g. [Special requirements and recommendations for data protection (PP) 1997].
6. GOST 29339-92. Informatsionnaya tekhnologiya. Zashchita informatsii ot utechki za schet pobochnykh elektromagnitnykh izlucheniy i navodok pri ee obrabotke sredstvami vychislitel'noy tekhniki. Obshchie tekhnicheskie trebovaniya [Information technology. Protection of information from leakage due to side electromagnetic radiation and interference in its processing by means of computer technology. General technical requirements].
7. *Parfenov V.I.* Zashchita informatsii. Slovar' [Information protection. Dictionary]. Voronezh, 2003, 292 p.
8. Sbornik metodicheskikh dokumentov FSTEK Rossii, 2005 [Collection of methodological documents of FSTEC of Russia, 2005].
9. *Khorev A.A.* Otsenka vozmozhnosti po perekhvatu pobochnykh elektromagnitnykh izlucheniy videosistemy komp'yutera. Ch. 2 [Evaluation of the possibility of intercepting side electromagnetic radiation of the computer video system. Part 2], *Spetsial'naya tekhnika* [Special equipment], 2011, No. 4.
10. Metodika PSAZ ot utechki za schet PEMIN raspredelennogo ob"ekta informatizatsii [PSAZ method from leakage due to pemin distributed object of Informatization].
11. Prikaz FSTEK Rossii ot 16 maya 2014 g. № 013 [Order of FSTEC of Russia of may 16, 2014 № 013].
12. *Ryzhenko S.V., Vasilenko V.V.* Uvelichenie zhiznennogo tsikla zashchishchennykh ob"ektov vychislitel'noy tekhniki za schet postroeniya prostranstvennoy sistemy aktivnoy zashchity informatsii raspredelennogo ob"ekta informatizatsii, obespechivayushchey zashchishchennost' po kanalu pobochnykh elektromagnitnykh izlucheniy ot osnovnykh tekhnicheskikh sredstv i sistem [Increasing the life cycle of protected objects of computer technology by building a spatial system of active protection of information distributed object of information, providing protection through the channel of electromagnetic radiation from the main technical means and systems], *Materialy XIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost' – 2015»* [Proceedings of the XIV International scientific and practical conference "Information security-2015"]. Taganrog, 2015.
13. *Kondrat'ev A.V.* Tekhnicheskaya zashchita informatsii. Praktika rabot po otsenke osnovnykh kanalov utechki [Technical protection of information. Practice of work on the assessment of the main leakage channels]. Moscow, 2016, 304 p.
14. *Kotenko V.V., Rumyantsev K.E.* Teoriya informatsii i zashchita telekommunikatsiy [Theory of information and protection of telecommunications]. Rostov-on-Don, 2009, 369 p.
15. *Sukharev E.M.* Obshchesistemnye voprosy zashchity informatsii [System - wide issues of information protection]. Moscow, 2003, 144 p.
16. *Takha Khemdi A.* Vvedenie v issledovanie operatsiy [Introduction to operations research]. Moscow, 2005, 912 p.

17. Prikaz FSTEK Rossii ot 20 oktyabrya 2016 g. № 025 [The order of FSTEC of Russia of October 20, 2016 № 025].
18. Kontrol' zashchishchennosti informatsii ot utechki po tekhnicheskim kanalam za schet pobochnykh elektromagnitnykh izlucheniy i navodok. Attestatsionnye ispytaniya po trebovaniyam bezopasnosti informatsii [Control of information security from leakage through technical channels due to side electromagnetic radiation and interference. Qualification tests according to the requirements of information security]. Modcow, 2014, 208 p.
19. *Sukharev E.M.* Modeli razvitiya tekhnicheskikh razvedok i ugroz bezopasnosti informatsii [Models of development of technical intelligence and threats to information security]. Moscow, 2003, 296 p.
20. *Vygodskiy M.Ya.* Spravochnik po vysshey matematike [Handbook of higher mathematics]. Moscow: Nauka, 1966.

Статью рекомендовал к опубликованию д.т.н., профессор С.М. Климов.

Василенко Владимир Васильевич – ООО «Центр безопасности информации»; e-mail: bsv@cbi-info.ru; Московская область, г. Королёв, мкр. Юбилейный, ул. Пионерская, д. ¼; тел.: 84955433060; д.т.н.; профессор; заместитель председателя.

Рыженко Сергей Викторович – e-mail: svr@cbi-info.ru; Московская область, г. Щёлково, ул. Центральная, д. 17, кв. 258; тел.: 84955433060, 89259229721; заместитель директора департамента специальных исследований.

Vasilenko Vladimir Vasil'evich – CLL "Center of Information Security"; e-mail: bsv@cbi-info.ru; Moscow region, Korolev, MD. Jubilee, Pionerskaya street, d. ¼; phone: +74955433060; dr. of eng. sc.; professor; deputy chairman.

Ryzhenko SergeyViktorovich – e-mail: svr@cbi-info.ru; Moscow region, Shchelkovo, Central street, 17, sq. 258; phones: +74955433060, +79259229721; deputy director of the department of special researches.

УДК 654.024:004.056 DOI 10.23683/2311-3103-2018-2-256-263

Firas Naziyah Mahmood, Hayder Hussein Shakir, K.Ye. Rumyantsev

SECURITY OF BANKING REMOTELY SYSTEM

SMS banking allows customers to request and receive banking information from their Bank on their mobile phones. Clients can securely manage their Bank accounts, balances of current account, send cheque requests and account fees. Secured banking channel SMS also acts as the means of the Bank alerting its customers, especially in an emergency situation. The aim of this paper to design and implement the program/ application to send and received a secured SMS for banking works, installing on client's devices by authorized bank employer. This program/Application decrypt the code that send to the client by one of the authorized telecommunication company servers according to contract with services provider company. The code expiration is 15 seconds for increasing the security levels and if the client doesn't send the code, the company send a new SMS to ask him to resend a new code, and we can make a limitation of the money Drawdowns per day according to dealing with the costumer contract with bank for increasing the level of security. IN case of using the card for drawdown more than the money that dealing with bank, the bank preform the locking procedure for that account and stopping the drawdown process and Report this situation from the customer of the bank that is under threat or other similar so. Electronic Markets (E-markets) can be more effective and less expensive way to sell products or provide services without geographical barriers. It changes the relationship of buyer-seller, improves business processes and helps reach new markets or segments through the electronic medium.

Banking Remotely; Security and Threats.