М.П. Сычев
доктор техн. наук, профессор
E-mail: zi@bmstu.ru
С.В. Скрыль
доктор техн. наук, профессор
В.О. Крылов
аспирант
Д.А. Холод
аспирант
О.С. Томах
ассистент кафедры
(Московский государственный технический университет им. Н.Э. Баумана)
г. Москва, Российская Федерация

Теоретические основания синтеза модели распознавания угроз утечки информации по параметрическим каналам в процессе управленческой деятельности

Анализируются недостатки существующей практики выявления параметрических каналов. Обосновывается актуальность проблемы разработки методических основ синтеза моделей распознавания угроз утечки информации по параметрическим каналам как фактора повышения эффективности выявления такого рода угроз. Формулируются и формально доказываются основополагающие положения об объективном характере проявления угроз утечки информации по параметрическим каналам в процессе управленческой деятельности и объективном характере мер комплексного технического контроля (КТК) защищенности информации от утечки, а также о структурированности признаков распознавания этих угроз, возникающих в результате их проявления. Указанные положения рассматриваются как основа теории синтеза модели распознавания угроз утечки информации по параметрическим каналам в процессе управленческой деятельности.

Ключевые слова: *утечка информации по параметрическим каналам; модель распознавания угроз утечки информации по параметрическим каналам; комплексный технический контроль защищенности информации от утечки по параметрическим каналам.*

M.P. Sychev
Doctor of Techn. Sciences, Professor
E-mail: zi@bmstu.ru
S.V. Skryl'
Doctor of Techn. Sciences, Professor
V.O. Krylov
Postgraduate Student
D.A. Kholod
Postgraduate Student
O.S.Tomakh
Assistant of the Department
(Bauman Moscow State Technical University)
Moscow, Russian Federation

Theoretical Foundations of the Synthesis of the Model of Recognizing the Threat of Information Leakage through Parametric Channels in the Management Process

The shortcomings of the existing practice of identifying p arametric channels are analyzed. The urgency of the problem of developing methodological foundations for the synthesis of models for detecting threats to leak information through parametric channels, as a factor in improving the effectiveness of identifying such threats, is substantiated. Formulating and formally proving fundamental provisions on the objective nature of the manifestation of threats of information leakage through parametric channels in the management process and the objective nature of the CTC's measures of information security against leakage, as well as on the structured recognition of signs of recognition of these threats resulting from their manifestation. These provisions are considered as the basis of the theory of synthesis of the model of recognition of threats to the leakage of information through parametric channels in the process of management.

Keywords: *leakage of information on parametric channels; model of detection of threats of information leakage on parametric channels; complex technical monitoring of information security on parametric channels.*

DOI: 10.25791/asu.08.2019.785

Значительный объем информации, используемый в процессе управленческой деятельности, дает предпосылку к возникновению целого ряда демаскирующих признаков, позволяющих определять характер такой деятельности [1]. Статус управленческой деятельности, как одной из наиболее информационно емких, делает ее объектом, представляющим огромный интерес для соответствующих субъектов, в виду возможности использования для достижения своих целей. Потенциальная возможность перехвата информации об управленческой деятельности обусловливает различного рода источники угроз утечки информации [2]. Этому способствуют следующие факторы:

- многообразие форм разведдеятельности [3];
- отсутствие адекватных механизмов ее предотвращения [4, 5];
- далекий от совершенства уровень развития методической базы для выявления признаков такого рода деятельности [6, 7];
- рост и постоянное совершенствование технической оснащенности субъектов разведдеятельности за счет использования новейших достижений научно-технического прогресса [8].

В этой связи следует отметить, что помещения органов управления, в которых установлены основные и вспомогательные технические средства и системы (ОТСС и ВТСС, соответственно), используемые в интересах информационной поддержки управленческой деятельности, а также внедренные в этих помещениях так называемые *полуактивные закладочные устройства* (ПЗУ) [1] являются источниками информативных электрических и электромагнитных сигналов, возникающих при изменении параметров технических средств (узлов), входящих в их состав. Существующая классификация технических каналов утечки информации определяет каналы подобного рода как параметрические.

Основными условиями возникновения параметрических каналов утечки информации в процессе управленческой деятельности являются изменения в поле информационного сигнала некоторых параметров (расстояния между деталями и проводниками и др.) технических средств (узлов, элементов и т. д.), содержащихся в составе ОТСС и (или) ВТСС, которые могут:

- модулировать информационными сигналами колебания внутренних генераторов этих средств;
- модулировать информационными сигналами колебания усилителей, входящих в состав этих средств и имеющих паразитную (авто) генерацию;
- модулировать информационными сигналами сторонние зондирующие ВЧ электромагнитные колебания по отходящим коммуникациям, имеющим выход за пределы контролируемой зоны;
- модулировать информационными сигналами сторонние зондирующие ВЧ электромагнитные поля;
- создавать за счет акустоэлектрических преобразований информационные электрические сигналы в отходящих коммуникациях, имеющих выход за пределы контролируемой зоны;
- использовать технические средства разведки на базе специальных высокочастотных генераторов, антенн, имеющих узкие диаграммы направленности, индукторов и специальных радиоприемных устройств для перехвата информации по каналам акустоэлектрических преобразований, ВЧ-облучения, паразитной (авто) генерации и ВЧ-навязывания.

В соответствии с работами [1, 8] эти условия относятся к источникам угроз утечки информации по параметрическим каналам.

Параметрические каналы утечки информации представляют существенную опасность вследствие сложности их обнаружения, обусловленной требованием проведения специальных мероприятий по оценке возможностей технических средств (узлов, элементов и т. д.) к формированию такого рода каналов.

Отсюда все более актуальной становится проблема обеспечения защиты информации от утечки по каналам данного вида. Результатом целенаправленного и системного применения технологий безопасности в этой области стало создание средств защиты информации от утечки по параметрическим каналам [9].

Вместе с тем совершенствование механизмов защиты информации от утечки по параметрическим каналам обусловило и адекватное совершенствование методов и средств преодоления этих механизмов. При этом, как показывает анализ состояния вопроса, темпы совершенствования способов и инструментов противоправных действий в сфере информационных технологий значительно превышают темпы совершенствования средств и способов защиты информации [10].

Главной причиной этого является традиционный подход к решению проблемы обнаружения такого рода источников угроз, основанный на выявлении лишь отдельных их признаков без какой-либо их систематизации [11].

Это обусловило анализ направлений совершенствования методов выявления утечки информации по параметрическим каналам в процессе управленческой деятельности как источника угроз нарушения ее конфиденциальности с целью обоснования путей совершенствования способов противодействия такого рода угрозам. Как показывает анализ, одним из таких направлений является использование в механизмах защиты информации компонентов обнаружения угроз нарушения конфиденциальности информации, построенных на основе теории распознавания [12…15].

Возможность применения методов данной теории основывается на установленных закономерностях в сценариях реализации нарушителем действий, связанных с перехватом информации по параметрическим каналам, позволяющих создать модель всех возможных действий, осуществляемых с целью доступа к конфиденциальной информации. Подобная модель является основой для реализации алгоритмов распознавания такого рода противоправных действий как источника угроз нарушения конфиденциальности информации и оценки уровня данных угроз информационной

безопасности управленческой деятельности, позволяющих не только выявлять признаки подобных действий, но и предложить способы и средства их идентификации [4, 5].

Все это в целом требует совершенствования методического обеспечения защиты конфиденциальной информации в процессе управленческой деятельности, что, в свою очередь, определяет необходимость решения научной проблемы разработки методических основ синтеза моделей распознавания угроз утечки информации по параметрическим каналам и позволяет повысить эффективность выявления такого рода угроз. Это приводит к необходимости разработки теории синтеза модели распознавания угроз утечки информации по параметрическим каналам в процессе управленческой деятельности.

Основополагающими положениями, лежащими в основе данной теории являются:

- положение об объективном характере проявления такого рода угроз (теоретическое положение 1);
- положение об объективном характере мер КТК защищенности информации от утечки (теоретическое положение 2);
- положение о структурированности признаков распознавания этих угроз, возникающих в результате их проявления (теоретическое положение 3).

Ниже приводятся формулировки и доказательства перечисленных теоретических положений.

Теоретическое положение 1. ***Угрозы утечки информации по параметрическим каналам в процессе управленческой деятельности носят объективный характер.***

Введем следующие обозначения:

$З^{(ид)} = \left\{ з_i^{(ид)} \right\}$, $i = 1,2,...,\left| з_i^{(ид)} \right|$ – множество закономерностей использования информации в процессе управленческой деятельности, способствующих возникновению угроз утечки информации по параметрическим каналам;

$З^{(ид)} = \left\{ з_j^{(ид)} \right\}$, $j = 1,2,...,\left| з_j^{(у)} \right|$ – множество закономерностей проявления такого рода угроз;

$С^{(ид)} = \left\{ c_{ij}^{(ид)} \right\}$ – множество соответствий элементов $З^{(ид)}$ элементам $З^{(у)}$. При этом значения элементов множества $С^{(ид)}$ определим исходя из условия:

$$c_{ij}^{(ид)} = \begin{cases} 1, \text{ если элемент } з_i^{(ид)} \text{ соответствует элементу } з_j^{(у)}; \\ 0, \text{ в противном случае.} \end{cases}$$

Теоретическое положение будем считать доказанным, если в матричном представлении множества $С^{(ид)}$ будет отсутствовать столбец, сумма значений которого равна 0.

Для доказательства данного теоретического положения воспользуемся аппаратом теории множеств [15] и установим соответствия между уязвимостями информации в процессе управленческой деятельности и проявлениями угроз утечки информации по параметрическим каналам. Определим состав множеств $З^{(ид)}$ и $З^{(у)}$ как областей отправления и прибытия соответствий.

Будучи по своей сути информационной, любая управленческая деятельность в силу разнообразия используемых ОТСС и ВТСС характеризуется уязвимостями к реализации угроз утечки информации по техническим каналам, включая параметрические каналы. Эти уязвимости будем рассматривать как закономерности возникновения такого рода угроз.

В соответствии с работами [6, 7] уязвимостями информации к реализации угроз ее утечки по параметрическим каналам в процессе управленческой деятельности являются:

- территориальная доступность объекта управления для ведения по ним технической разведки, $з_1^{(ид)}$;
- наличие в помещениях объекта управления труб отопления, водоснабжения, газоснабжения, кабелей электропитания, $з_2^{(ид)}$;
- наличие на объекте управления радиосети, $з_3^{(ид)}$;
- наличие в помещениях объекта управления охранно-пожарной сигнализации, $з_4^{(ид)}$;
- наличие в помещениях объекта управления бытовой техники, $з_5^{(ид)}$;
- наличие в помещениях объекта управления сети электрочасов, $з_6^{(ид)}$;
- наличие в помещениях объекта управления трансляционной сети и громкоговорящей связи, $з_7^{(ид)}$;
- наличие на объекте управления внешней телефонной связи, $з_8^{(ид)}$;
- наличие в помещениях объекта управления линий связи, $з_9^{(ид)}$;
- наличие на объекте управления работающих ОТСС, $з_{10}^{(ид)}$;
- наличие на объекте управления работающих ВТСС, $з_{11}^{(ид)}$;
- выход кабелей питания и цепей заземления СВТ за пределы помещений объекта управления, $з_{12}^{(ид)}$;
- превышение уровня ЭМИ на частотах работы ВЧ генераторов ОТСС и ВТСС на границе территории объекта управления допустимой величины, $з_{13}^{(ид)}$;
- превышение уровня ЭМИ на частотах самовозбуждения усилителей НЧ ВТСС на границе территории объекта управления допустимой величины, $з_{14}^{(ид)}$;
- наличие зданий напротив окон помещений объекта управления, откуда возможно осуществлять перехват информации, $з_{15}^{(ид)}$.

Основными объективными закономерностями проявления угроз утечки информации по параметрическим каналам в процессе управленческой деятельности являются ниже перечисленные возможности перехватов:

- электромагнитных сигналов колебаний внутренних генераторов, входящих в состав ОТСС и (или) ВТСС, модулированных информационными сигналами, $з_1^{(у)}$;
- электромагнитных сигналов колебаний усилителей, входящих в состав ОТСС и (или) ВТСС, модулированных информационными сигналами, $з_2^{(у)}$;
- электромагнитных сигналов колебаний технических средств (узлов, элементов и т. д.), имеющих

паразитную (авто) генерацию, входящих в состав ОТСС и (или) ВТСС, модулированных информационными сигналами, $з_3^{(y)}$;

- переизлученных электромагнитных сигналов технических средств (узлов, элементов и т. д.), входящих в состав ОТСС и (или) ВТСС, которые могут модулировать информационными сигналами сторонние зондирующие ВЧ электромагнитные поля, $з_4^{(y)}$;
- электрических сигналов в токопроводящих линиях, выходящих за пределы территории объекта управления, модулированных информационными сигналами и излучаемых техническими средствами (узлами, элементами и т. д.), входящими в состав ОТСС и (или) ВТСС под воздействием сигналов сторонних зондирующих ВЧ электромагнитных полей, $з_5^{(y)}$;
- электрических сигналов в токопроводящих линиях, выходящих за пределы территории объекта управления, модулированных информационными сигналами средствами (узлами, элементами и т. д.), входящими в состав ОТСС и (или) ВТСС под воздействием сторонних «навязанных» зондирующих ВЧ электрических сигналов, $з_6^{(y)}$;
- электрических сигналов в токопроводящих линиях, выходящих за пределы территории объекта управления, модулированных информационными сигналами и излучаемых техническими средствами (узлами, элементами и т. д.), входящими в состав ОТСС и (или) ВТСС из-за эффекта акустоэлектрических преобразований, $з_7^{(y)}$.

Определим множество $C^{(uд)}$ соответствий элементов множества $З^{(y)}$ элементам множества $З^{(uд)}$. Для этого определим факт возможности использования i-й уязвимости информации для реализации j-й угрозы утечки информации по параметрическим каналам. В матрице, представленной на рисунке 1, приводятся результаты анализа такого рода возможностей. Столбцы матрицы соответствуют индексам элементов множества $З^{(uд)}$, а строки – индексам элементов множества $З^{(y)}$.

Из представленной на рисунке 1 матрицы очевидно, что в ней отсутствуют столбцы, сумма значений которых равна 0. Это является доказательством данного теоритического положения.

Теоретическое положение 2. ***Меры комплексного технического контроля защищенности информации от утечки по параметрическим каналам в процессе управленческой деятельности носят объективный характер.***

Введем следующие обозначения:

$З^{(KTK)} = \left\{ з_k^{(KTK)} \right\}$, $k = 1, 2, ..., \left| з_k^{(KTK)} \right|$ – множество закономерностей по реализации мер КТК в процессе управленческой деятельности;

$C^{(KTK)} = \left\{ c_{jk}^{(KTK)} \right\}$ – множество соответствий элементов $З^{(y)}$ элементам $З^{(KTK)}$. При этом значения элементов множества $C^{(KTK)}$ определим исходя из условия:

$$c_{jk}^{(KTK)} = \begin{cases} 1, & \text{если элемент } з_j^{(y)} \text{ соответствует элементу } з_k^{(KTK)}; \\ 0, & \text{в противном случае.} \end{cases}$$

Как и в предыдущем случае, теоретическое положение будем считать доказанным, если в матричном представлении множества $C^{(KTK)}$ будет отсутствовать столбец, сумма значений которого равна 0.

Для доказательства данного теоретического положения установим соответствия между угрозами утечки информации по параметрическим каналам и мерами КТК, направленных на выявление угроз данного типа. Определим состав множеств $З^{(y)}$ и $З^{(KTK)}$ как областей отправления и прибытия соответствий.

Меры КТК в любом органе управления, в силу разнообразия используемых средств контроля, характеризуются возможностями выявления угроз утечки информации по параметрическим каналам. Эти возможности будем рассматривать как объективные закономерности выявления такого рода угроз.

В соответствии с работами [4, 5] к мерам КТК защищенности информации от утечки по параметрическим каналам в процессе управленческой деятельности следует отнести:

- автоматизированное получение параметров тестовых электрических сигналов для последующей

	$з_1^{(uд)}$	$з_2^{(uд)}$	$з_3^{(uд)}$	$з_4^{(uд)}$	$з_5^{(uд)}$	$з_6^{(uд)}$	$з_7^{(uд)}$	$з_8^{(uд)}$	$з_9^{(uд)}$	$з_{10}^{(uд)}$	$з_{11}^{(uд)}$	$з_{12}^{(uд)}$	$з_{13}^{(uд)}$	$з_{14}^{(uд)}$	$з_{15}^{(uд)}$
$з_1^{(y)}$	1	0	1	1	1	0	0	0	0	1	1	0	1	1	1
$з_2^{(y)}$	1	0	1	1	1	0	0	0	0	1	1	0	1	1	1
$з_3^{(y)}$	1	0	1	1	1	0	0	0	0	1	1	0	1	1	1
$з_4^{(y)}$	1	0	1	1	1	0	0	0	0	1	1	0	1	1	1
$з_5^{(y)}$	1	1	0	1	1	1	1	1	1	1	1	1	0	0	0
$з_6^{(y)}$	1	1	0	1	1	1	1	1	1	1	1	1	0	0	0
$з_7^{(y)}$	1	1	0	1	1	1	1	1	1	1	1	1	0	0	0

Рис. 1. Анализ возможности использования i-й уязвимости информации для реализации j-й угрозы утечки информации по параметрическим каналам

оценки защищенности акустической информации объектов управления от утечки по каналу акустоэлектрических преобразований, $з_1^{(КТК)}$;

- автоматизированное получение параметров переизлученных тестовых сигналов для последующей оценки защищенности акустической информации объектов управления от утечки по каналу ВЧ-облучения, $з_2^{(КТК)}$;
- автоматизированное получение параметров тестовых электрических сигналов для последующей оценки защищенности акустической информации объектов управления от утечки по каналу ВЧ-навязывания, $з_3^{(КТК)}$;
- автоматизированное получение параметров тестовых электромагнитных сигналов для последующей оценки защищенности акустической информации объектов управления от утечки по каналам паразитной (авто) генерации, $з_4^{(КТК)}$;
- анализ защищенности акустической информации объектов управления от утечки по каналам акустоэлектрических преобразований, ВЧ-облучения, паразитной (авто) генерации и ВЧ-навязывания, $з_5^{(КТК)}$.

Определим множество $C^{(КТК)}$ соответствий элементов множества $З^{(у)}$ элементам множества $З^{(КТК)}$. Для этого определим факт возможности выявления *j*-й угрозы утечки информации по параметрическим каналам при реализации *k*-й меры КТК. В матрице, представленной на рисунке 2, приводятся результаты анализа такого рода возможностей. Столбцы матрицы соответствуют индексам элементов множества $З^{(КТК)}$, а строки – индексам элементов множества $З^{(у)}$.

Из представленной на рисунке 2 матрицы очевидно, что в ней отсутствуют столбцы, сумма значений которых равна 0. Это является доказательством данного теоритического положения.

Теоретическое положение 3. ***Множество признаков распознавания угроз утечки информации по параметрическим каналам в процессе управленческой деятельности является структурированным.***

	$з_1^{(КТК)}$	$з_2^{(КТК)}$	$з_3^{(КТК)}$	$з_4^{(КТК)}$	$з_5^{(КТК)}$
$з_1^{(у)}$	0	0	0	1	1
$з_2^{(у)}$	0	0	0	1	1
$з_3^{(у)}$	0	0	0	1	1
$з_4^{(у)}$	0	0	0	1	1
$з_5^{(у)}$	0	1	0	0	1
$з_6^{(у)}$	0	0	1	0	1
$з_7^{(у)}$	1	0	0	0	1

Рис. 2. Анализ возможности выявления j-й угрозы утечки информации по параметрическим каналам при реализации k-й меры КТК

Исходя из функционального характера действий по перехвату информации по параметрическим каналам, признаки такого рода действий также носят функциональный характер.

С целью представления множества признаков действий по перехвату информации по параметрическим каналам как признаков распознавания соответствующих угроз ее безопасности, воспользуемся методологическим аппаратом системного анализа. В соответствии с основополагающими принципами системного анализа в проблематике технической защиты информации [12] и существующими взглядами на пути решения проблемы распознавания угроз ее безопасности [14] исследование такого рода процессов как перехват информации по параметрическим каналам проводится с использованием сценарных описаний, отражающих различные аспекты этих процессов как объекта исследования.

Сценарное представление, как инструмент описания исследуемого вида деятельности, должно отражать совокупность действий над объектом исследования, именуемых *процедурными знаниями*.

Анализ общенаучного понятия «описание», позволяет установить присутствие в нем семантического аспекта, заключающегося в формировании множества данных о сущности описываемого объекта, отражающего некоторый образ действий, в той или иной степени подобный исследуемым.

Исходя из того, что семантика такого объекта как процесс перехвата информации по параметрическим каналам предполагает наличия у данного рода угроз источника – нарушителя, то семантично связанным и первичным по характеру причинно-следственных связей будет процесс «перехват информации по параметрическим каналам». Следовательно, для обоснования требований к моделям распознавания такого рода угрозам необходимо сформировать описание действий по их реализации.

Как показывает опыт проведения ряда исследований с целью криминалистического описания противоправных действий в информационной сфере, выполненных на основе методологии системного анализа [10], а также их формализованного представления, выполненных на основе методологии математического моделирования [16, 17], весьма результативным способом функционального представления угроз утечки информации по параметрическим каналам как объекта распознавания является представлением в виде направленных графов.

Структурирование описания противоправных действий по перехвату информации по параметрическим каналам связанно с достаточно ограниченным изучением общей картины подобного рода действий и исследованием содержания их внутренних связей. В этих целях используется методология структурного анализа.

Структурным анализом принято называть метод исследования, который начинается с общего обзора

объекта исследования с последующей детализацией знаний об объекте, в результате отраженные в описании объекта знания о нем представляются в виде иерархической структуры [18], число уровней которой зависит от глубины детализации. Структурирование по отношению к формальным методам описания является инструментом первичной формализации исследуемого объекта, позволяющим существенно снизить сложность его описания. Вместе с тем структурирование трудно формализуемых процессов, к которым относятся и действия по перехвату информации по параметрическим каналам носят эвристический характер.

Принимая во внимание целевую направленность такого рода действий, при их исследовании методами структурного анализа, структурированию подлежит целевая функция противоправных действий, что влечет за собой необходимость выделения в процессе структурирования функционально специализированных элементов. При этом в результате спецификации функций противоправных действий и образующихся при их реализации логических связей формируется функциональное представление такого рода действий в виде той или иной формы описания их функциональной структуры [19]. Представленная в терминах такого описания структура противоправных действий является структурным базисом целевой функции «Действия по перехвату информации по параметрическим каналам».

Структурированное функциональное представление такого рода действий позволяет [20]:

- отобразить в полном объеме все существенные элементы противоправных действий и их взаимосвязи;
- воспроизвести все их значимые характеристики;
- обеспечить унифицированность описания структуры и взаимосвязей между элементами на любом уровне структуризации целевой функции.

Эвристический характер структурных методологий накладывает ряд ограничений на их применение для анализа действий по перехвату информации по параметрическим каналам. Эти ограничения связаны со сложностью спецификации отдельных функционально специализированных элементов рассматриваемого вида деятельности. Вместе с тем лишь структурные методологии дают возможность предоставить достаточный инструментарий для описания процессов такого уровня сложности, как рассматриваемые.

Таким образом, функциональное описание действий по перехвату информации по параметрическим каналам представляет собой систему функций, выполняемых в процессе реализации угроз утечки информации по каналам рассматриваемого типа. Подобное функциональное описание формируется на основе [20]:

- экспертных знаний о специфике противоправных действий по перехвату информации по параметрическим каналам;
- формальных правил, интерпретирующих эти знания;
- формы представления описания, термины которой соответствуют процедуре анализа.

В основу процедур формирования функционального описания действий по перехвату информации по параметрическим каналам положены два основных принципа: нисходящий способ структуризации целевой функции и обоснованность степени ее детализации.
Согласно первому принципу информация об особенностях действий по перехвату информации по параметрическим каналам иерархически распределяется по уровням, постепенно детализируется и уточняется.

Исходя из того, что степень достижения нарушителем поставленных целей по реализации угроз утечки информации по параметрическим каналам характеризуется его целевой функцией, то очевидно, что и в отношении как целевой функции, так и в отношении ее компонент допускается функциональное представление. В свою очередь, допустимость функционального представления рассматриваемого вида действий предполагает представление их совокупностью действий нарушителя, реализация которых обеспечивает достижение цели. При этом совокупность действий нарушителя является упорядоченной, а сам порядок отражает алгоритм действий.

Таким образом, представление целевой функции «Действия по перехвату информации по параметрическим каналам» в виде упорядоченной последовательности действий нарушителя и лежит в основе ее структуризации. При этом следует учесть, что множественность функционального представления цели такого рода действий допускает не один, а множество вариантов структуризации целевой функции, количество которых ограничивается требуемым уровнем структуризации.

В соответствии со вторым принципом достигается необходимая степень детализации целевой функции «Действия по перехвату информации по параметрическим каналам».

Практика функционального моделирования информационных процессов, включая процессы реализации угроз информационной безопасности, позволила обосновать ряд эвристических правил, в соответствии с которыми детализация функционального описания исследуемого процесса считается достаточной, если вариант структуризации:

1) однозначно определяет исполнителя подобного рода действий – непосредственно нарушитель либо используемое им средство;

2) обеспечивает достоверное представление функциональных связей;

3) представляет специфицируемые функции как криминалистически значимые признаки такого рода противоправных действий.

В соответствии с целью действий по перехвату информации по параметрическим каналам их результатом является реализация целевой функции $\Phi^{(0)}$. Индекс 0 указывает на представление верхнего (нулевого) уровня структуры функционального описания, так как целевая функция соответствует концептуальному (обобщенному) функциональному представлению

исследуемого процесса. Это позволяет реализовать унифицированный методический аппарат для формирования функциональных моделей рассматриваемого вида действий для любой степени их детализации.

Допустимость функционального представления цели действий нарушителя по перехвату информации по параметрическим каналам предполагает наличие множества такого рода действий, последовательная реализация которых составляет целевую функцию $\Phi^{(0)}$. В свою очередь, эти действия могут быть представлены в виде определенной последовательности операций.

Представление целевой функции $\Phi^{(0)}$ действий в виде упорядоченных последовательностей воздействий $\phi_l^{(1)} \in \Phi^{(0)}$ составляет процесс ее декомпозиции. Следует отметить, что речь идет о декомпозиции функционального представления, порождающего соответствующие уровни иерархии, в данном случае – декомпозиции обобщенного (нулевого) уровня на следующий, первый уровень.

Из изложенного следует, что множество признаков распознавания угроз утечки информации по параметрическим каналам является структурированным.

Сформулированные теоретические основания синтеза модели распознавания угроз утечки информации по параметрическим каналам в процессе управленческой деятельности позволяют разработать системы распознавания такого рода угроз безопасности информации, обеспечивающие существенное повышение эффективности их выявления.

Список литературы

1. Меньшаков Ю.К. *Основы технических разведок*: учебник / Под ред. М.П. Сычева. М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. 478 с.
2. Хорев А.А. *Техническая защита информации*: учебное пособие для студентов вузов. Том 1. Технические каналы утечки информации / Под ред. Ю.Н. Лаврухина. М.: НПЦ «Аналитика», 2008. 436 с.
3. Меньшаков Ю.К. *Виды и средства иностранных технических разведок*: учебник / Под ред. М.П. Сычева. М.. Изд-во МГТУ им. Н.Э. Баумана, 2009. 656 с.
4. Чекалин А.А., Скрыль С.В., Минаев В.А., Хохлов Н.С., Бокова О.И. [и др.]. *Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел*: учебное пособие для высших учебных заведений МВД России. Ч. 2: Практические аспекты технической разведки и комплексного технического контроля. М.: Горячая линия-Телеком, 2006. 205 с.
5. Чекалин А.А., Скрыль С.В., Минаев В.А., Хохлов Н.С., Бокова О.И. [и др.]. *Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел*: учебное пособие для высших учебных заведений МВД России. Ч. 1: Теоретические основы технической разведки и комплексного технического контроля М.: Горячая линия-Телеком, 2006. 313 с.
6. ФСТЭК России. *Нормативно-методический документ. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры.* М: ОАО «Типография МВД», 2007. 44 с.
7. ФСТЭК России. *Руководящий документ. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры.* М: ОАО «Типография МВД», 2007. 145 с.
8. Скрыль С.В., Шелупанов А.А. [и др]. *Технические средства и методы защиты информации*: учебник для студентов высших учебных заведений. М.: Машиностроение, 2008. 508 с.
9. Новокшанов И.В. [и др.]. *Информационная безопасность телекоммуникационных систем (технические вопросы)*: учебное пособие для системы высшего профессионального образования России. М.: Радио и связь, 2004. 388 с.
10. Скрыль С.В., Шелупанов А.А. *Основы системного анализа в защите информации*: учебное пособие для студентов высших учебных заведений. М.: Машиностроение, 2008. 138 с.
11. Горелик А.Л., Скрипкин В.А. *Методы распознавания*: учебное пособие для вузов. М.: Высшая школа, 1977. 222 с.
12. Фу К. *Структурные методы в распознавании образов*: пер. с англ. М.: Мир, 1977. 319 с.
13. Фукунага К. *Введение в статистическую теорию распознавания образов*: пер. с англ. М.: Наука, 1979. 368 с.
14. Киселев В.В. *Распознавание и оценка угроз информационной безопасности территориальным сегментам единой информационно-телекоммуникационной системы органов внутренних дел: теоретические и организационно-методические основы*: монография. Воронеж: Воронежский институт МВД России, 2012. 160 с.
15. Александров П.С. *Введение в теорию множеств и общую топологию*. М.: Наука, 1977. 368 с.
16. Советов Б.Я., Яковлев С.А. *Моделирование систем*: учебник для вузов. 3-е изд., перераб. и доп. М.: Высшая школа, 2001. 343 с.
17. Скрыль С.В., Крылов В.О., Филева С.А., Гуляев О.А. Функциональное представление угроз утечки информации по виброакустическим каналам на объектах авиакосмической промышленности // *Авиакосмическое приборостроение*. М.: Научтехлитиздат. 2017, № 12. С. 22–32.
18. Месарович М., Мако Д., Такахара И. *Теория иерархических многоуровневых систем*. М.: Мир, 1973. 344 с.
19. Скрыль С.В., Малышев А.А., Волкова С.Н., Герасимов А.А. *Функциональное моделирование как методология исследования конфиденциальности информационной деятельности* // Интеллектуаль-

ные системы: Труды Девятого международного симпозиума. М.: РУСАКИ, 2010. С. 590–593.
20. Калянов Г.Н. *CASE: Структурный системный анализ (автоматизация и применение)*. М.: Лори, 1996. 242 с.

References

1. Menshakov Yu.K. *Osnovy tekhnicheskikh razvedok*: uchebnik / Pod red. M.P. Sycheva [Basics of technical intelligence: a textbook. Edited by M.P. Sychev]. M.: Izd-vo MGTU im. N.E. Baumana [Moscow: Publishing house «Moscow State Technical University named after N.E. Bauman»]. 2011. 478 p.
2. Khorev A.A. *Tekhnicheskaya zashchita informatsii*: uchebnoe posobie dlya studentov vuzov. Tom 1. Tekhnicheskie kanaly utechki informatsii / Pod red. Yu.N. Lavrukhina [Technical protection of information: a textbook for university students. Vol. 1: Technical channels of information leakage. Edited by Yu.N. Lavruhin]. M.: NPTs «Analitika» [Moscow: SPC «Analytics»]. 2008. 436 p.
3. Menshakov Yu.K. *Vidy i sredstva inostrannykh tekhnicheskikh razvedok*: uchebnik / Pod red. M.P. Sycheva [Types and means of foreign technical intelligence: a textbook. Edited by M.P. Sychev]. M.. Izd-vo MGTU im. N.E. Baumana [Moscow: Publishing house «Moscow State Technical University named after N.E. Bauman»]. 2009. 656 p.
4. Chekalin A.A., Skryl' S.V., Minaev V.A., Khokhlov N.S., Bokova O.I. [et al.]. *Kompleksnyy tekhnicheskiy kontrol effektivnosti mer bezopasnosti sistem upravleniya v organakh vnutrennikh del*: uchebnoe posobie dlya vysshikh uchebnykh zavedeniy MVD Rossii. Ch. 2: Prakticheskie aspekty tekhnicheskoy razvedki i kompleksnogo tekhnicheskogo kontrolya [Integrated technical control of the effectiveness of security measures of management systems in internal affairs bodies: a textbook for higher educational institutions of the Ministry of Internal Affairs of Russia. Part 2: Practical aspects of technical reconnaissance and integrated technical control]. M.: Goryachaya liniya-Telekom [Moscow: Publishing house «Hot line-Telecom»]. 2006. 205 p.
5. Chekalin A.A., Skryl' S.V., Minaev V.A., Khokhlov N.S., Bokova O.I. [et al.]. *Kompleksnyy tekhnicheskiy kontrol effektivnosti mer bezopasnosti sistem upravleniya v organakh vnutrennikh del*: uchebnoe posobie dlya vysshikh uchebnykh zavedeniy MVD Rossii. Ch. 1: Teoreticheskie osnovy tekhnicheskoy razvedki i kompleksnogo tekhnicheskogo kontrolya [Integrated technical control of the effectiveness of security measures of management systems in internal affairs bodies: a textbook for higher educational institutions of the Ministry of Internal Affairs of Russia. Part 1: Theoretical basis of technical intelligence and integrated technical control]. M.: Goryachaya liniya-Telekom [Moscow: Publishing house «Hot line-Telecom»]. 2006. 313 p.
6. FSTEK Rossii. *Normativno-metodicheskiy dokument. Metodika opredeleniya aktualnykh ugroz bezopasnosti informatsii v klyuchevykh sistemakh informatsionnoy infrastruktury* [Federal Service for Technical and Export Control: Regulatory and procedural document. Methods for determining the actual threats to the security of information in key information infrastructure systems]. M: OAO «Tipografiya MVD» [Moscow: JSC «Printing house of the Ministry of Internal Affairs»]. 2007. 44 p.
7. FSTEK Rossii. *Rukovodyashchiy dokument. Bazovaya model ugroz bezopasnosti informatsii v klyuchevykh sistemakh informatsionnoy infrastruktury* [Federal Service for Technical and Export Control: Guidance document. The basic model of information security threats in key information infrastructure systems]. M: OAO «Tipografiya MVD» [Moscow: JSC «Printing house of the Ministry of Internal Affairs»]. 2007. 145 p.
8. Skryl' S.V., Shelupanov A.A. [et al.]. *Tekhnicheskie sredstva i metody zashchity informatsii*: uchebnik dlya studentov vysshikh uchebnykh zavedeniy [Technical means and methods of information protection: a textbook for students of higher educational institutions]. M.: Mashinostroenie [Moscow: Publishing house «Engineering»]. 2008. 508 p.
9. Novokshanov I.V. [et al.]. *Informatsionnaya bezopasnost telekommunikatsionnykh sistem (tekhnicheskie voprosy)*: uchebnoe posobie dlya sistemy vysshego professionalnogo obrazovaniya Rossii [Information security of telecommunication systems (technical issues): A manual for the system of higher professional education in Russia]. M.: Radio i svyaz [Publishing house «Radio and communication»]. 2004. 388 p.
10. Skryl' S.V., Shelupanov A.A. *Osnovy sistemnogo analiza v zashchite informatsii*: uchebnoe posobie dlya studentov vysshikh uchebnykh zavedeniy [Fundamentals of system analysis in the protection of information: a manual for students of higher educational institutions]. M.: Mashinostroenie [Moscow: Publishing house «Engineering»]. 2008. 138 p.
11. Gorelik A.L., Skripkin V.A. *Metody raspoznavaniya*: uchebnoe posobie dlya vuzov [Recognition methods: a textbook for universities]. M.: Vysshaya shkola [Moscow: Publishing house «High School»]. 1977. 222 p.
12. Fu K. Strukturnye metody v raspoznavanii obrazov: per. s angl. []. M.: Mir [Moscow: Publishing house «Engineering»]. 1977. 319 p.
13. Fukunaga K. Vvedenie v statisticheskuyu teoriyu raspoznavaniya obrazov: per. s angl.[]. M.: Nauka [Moscow: Publishing house «Engineering»]. 1979. 368 p.
14. Kiselev V.V. *Raspoznavanie i otsenka ugroz informatsionnoy bezopasnosti territorialnym segmentam edinoy informatsionno-telekommunikatsionnoy sistemy organov vnutrennikh del*: teoreticheskie i organizatsionno-metodicheskie osnovy: monografiya [Recognition and assessment of information security threats to territorial segments of a unified information and telecommunication system of internal affairs bodies: theoretical, organizational and methodological foundations: monograph].

Voronezh: Voronezhskiy institut MVD Rossii [Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia]. 2012. 160 p.
15. Aleksandrov P.S. *Vvedenie v teoriyu mnozhestv i obshchuyu topologiyu* [Introduction to set theory and general topology]. M.: Nauka [Moscow: Publishing house «Science»]. 1977. 368 p.
16. Sovetov B.Ya., Yakovlev S.A. *Modelirovanie sistem*: uchebnik dlya vuzov. 3-e izd., pererab. i dop. [Modeling of systems: textbooks for universities (3rd ed., revised and additional)]. M.: Vysshaya shkola [Moscow: Publishing house «High School»]. 2001. 343 p.
17. Skryl' S.V., Krylov V.O., Fileva S.A., Gulyaev O.A. *Funktsionalnoe predstavlenie ugroz utechki informatsii po vibroakusticheskim kanalam na obektakh aviakosmicheskoy promyshlennosti* [Functional presentation of threats of information leakage through vibro-acoustic channels at aerospace objects]. *Aviakosmicheskoe priborostroenie* [Aerospace Instrumentation]. 2017, no. 12, pp. 22–32.
18. Mesarovich M., Mako D., Takakhara I. *Teoriya ierarkhicheskikh mnogourovnevykh system* [Theory of hierarchical multi-level systems]. M.: Mir [Moscow: Publishing house «Peace»]. 1973. 344 p.
19. Skryl' S.V., Malyshev A.A., Volkova S.N., Gerasimov A.A. Funktsionalnoe modelirovanie kak metodologiya issledovaniya konfidentsialnosti informatsionnoy deyatelnosti. *Intellektualnye sistemy: Trudy Devyatogo mezhdunarodnogo simpoziuma* [Functional modeling as a methodology for researching information activities]. M.: RUSAKI [Moscow: Publishing house «RUSAKI»]. 2010, pp. 590–593.
20. Kalyanov G.N. *CASE: Strukturnyy sistemnyy analiz (avtomatizatsiya i primenenie)* [CASE: Structural system analysis (automation and application)]. M.: Lori [Moscow: Publishing house «Lori»]. 1996. 242 p.

Информация об авторах

Сычев Михаил Павлович, доктор технических наук, профессор, профессор кафедры защиты информации (ИУ-10)
E-mail: zi@bmstu.ru
Скрыль Сергей Васильевич, доктор технических наук, профессор, профессор кафедры защиты информации (ИУ-10)
Крылов Владислав Олегович, аспирант кафедры защиты информации (ИУ-10)
Холод Денис Александрович, аспирант кафедры защиты информации (ИУ-10)
Томах Олеся Сергеевна, ассистент кафедры защиты информации (ИУ-10)
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет им. Н.Э. Баумана»
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5

Information about the authors

Sychev Mikhail Pavlovich, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security
E-mail: zi@bmstu.ru
Skryl' Sergey Vasilevich, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security
Krylov Vladislav Olegovich, Postgraduate Student of the Department of Information Security
Kholod Denis Aleksandrovich, Postgraduate Student of the Department of Information Security
Tomakh Olesya Sergeevna, Assistant of the Department of Information Security
Federal State Educational Institution of Higher Education «Bauman Moscow State Technical University»
105005, Russian Federation, Moscow, str. 2nd Bauman, 5