13. *Salal Y.K., Abdullaev S.M.* Optimization of Classifiers Ensemble Construction: Case Study of Educational Data Mining, *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2019, Vol. 19, No. 4, pp. 139-143. DOI: 10.14529/ctcr190414
14. *Salal Y.K., Abdullaev S.M., Mukesh Kumar*. Educational Data Mining: Student Performance Prediction in Academic, *Inter. Journal of Engineering and Advanced Technology (IJEAT)*, April 2019, Vol. 8 (4) ,pp. 54-59.
15. *Salal Y.K., Abdullaev S.M.* Educational data mining using base and ensemble Learning approaches to predict student's performance. *Informatizaciya-i-Svyaz*, 2019, No. 5, pp.140-143.
16. *Chawla N.V.* Data mining for imbalanced datasets: An overview, Data Mining and Knowledge Discovery Handbook, Springer. Boston, MA, 2010, pp. 875-886. DOI: 10.1007/978-0-387-09823-4_455.
17. *Galar, M., Fernandez, A., Barrenechea, E., Bustince, H. and Herrera, F.* X A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches, *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 2011, Vol. 42 (4), pp. 463-484. DOI: 10.1109/TSMCC.2011.2161285.
18. *Hartshorne J.K. and Germine L.T.* When does cognitive functioning peak? The asynchronous rise and fall of different cognitive abilities across the life span, *Psychological science*, 2015, Vol. 26 (4), pp. 433-443. DOI:10.1177/0956797614567339.
19. *Abdullaev S.M., Lenskaya O.Yu., Salal Ya.K.* Computer Systems of Individual Instruction: Features of Student Model, *Proceedings of the IV international scientific and practical conference, October 11-12, 2018, Chelyabinsk*, pp. 7-14. (in Russ.).
20. *González P., Castaño A., Chawla N.V., Coz J.J.D.* A review on quantification learning, *ACM Computing Surveys (CSUR)*, 2017, Vol. 50, No. 5, pp. 1-40. DOI: 10.1145/311780.
21. *Forman G.* Quantifying counts and costs via classification, *Data Mining and Knowledge Discov*, 2008, Vol. 17, No. 2, pp. 164-206. DOI: 10.1007/s10618-008-0097-y.

Статью рекомендовала к опубликованию к.т.н. О.Ю. Ленская.

Салал Ясс Кхудейр – Южно-Уральский государственный университет (национальный исследовательский университет); e-mail: Yasskhudheirsalal@gmail.com; г. Челябинск, просп. Ленина, 76; кафедра системного программирования; аспирант.

Абдуллаев Санжар Муталович – e-mail: abdullaevsm@susu.ru; кафедра системного программирования; д. геогр. н.; профессор.

Salal Yass Khudheir – South Ural State University; e-mail: Yasskhudheirsalal@gmail.com; 76, Lenin prospect, Chelyabinsk, 454080, Russia; the department of system programming; postgraduate student.

Abdullaev Sanjar Mutalovich – e-mail: abdullaevsm@susu.ru; the department of system programming; dr. of geogr. sc.; professor.

УДК 004.056.5 DOI 10.18522/2311-3103-2020-3-122-132

П.А. Чуб, Д.Н. Цветкова, Н.В. Болдырихин, Д.А. Короченцев

ОЦЕНКА ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ ОТ УТЕЧЕК РЕЧЕВОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ШУМОВ

Рассматриваются особенности применения методик аттестации защищенных помещений. Такие методики разрабатываются и регламентируются Федеральной службой по техническому и экспортному контролю. Необходимость аттестации связана с наличием технических каналов утечки информации, по которым злоумышленником могут быть получены сведения, составляющие коммерческую, государственную или иную тайну. Наличие технических каналов утечки информации обусловлено физическими процессами, связанными с особенностями распространения акустических, электромагнитных и оптических

волн. Через такие каналы возможна утечка акустической, видовой информации, информации, обрабатываемой техническими средствами и системами. В рамках данной работы рассматриваются особенности аттестации защищенных помещений от утечек акустической информации. Аттестация включает в себя проведение инструментальных измерений, которые позволяют обнаружить информативный сигнал в линиях связи, в эфире, в системах отопления, водопровода, вентиляции и т.д. Помимо измерений аттестация предполагает проведение расчетов, на основании которых делается вывод о соответствии или несоответствии уровня защищенности. Расчетная часть является довольно громоздкой и сложной, поэтому целью работы является разработка алгоритма, который позволяет определить степень защищенности выделенного помещения от утечки речевой информации. Задачами работы являются: разработка вспомогательных алгоритмов для расчета параметров защищенности помещения по каждому типу каналов утечки речевой информации; реализация программного средства, позволяющего определить степень защищенности помещения; проведение исследования зависимости защищенности помещения от уровня шумов с использованием разработанного программного средства. В качестве результатов работы следует отметить синтезированный алгоритм и разработанное программное средство, позволяющее существенно сократить время на процедуру оценки защищенности помещения и избежать ошибок. Так же результатом работы является исследование зависимости словесной разборчивости речи от уровня шумов в различных октавах. Исследования показали, что словесная разборчивость, которая определяет защищенность помещения по акустическим параметрам, нелинейно спадает с увеличением уровня шумов при фиксированном уровне сигнала.

Информационная безопасность; утечка речевой информации; выделенное помещение; канал утечки информации; оценка защищенности помещения.

P.A. Chub, D.N. Tsvetkova, N.V. Boldyrikhin, D.A. Korochentsev

ESTIMATION OF SECURITY OF THE PREMISES FROM LEAKAGE OF SPEECH INFORMATION IN CONDITIONS OF EXPOSURE TO NOISE

The article discusses the features of the application of certification methods for protected premises. Such techniques are developed and regulated by the Federal Service for Technical and Export Control. The need for certification is associated with the presence of technical channels for information leakage, through which an attacker can obtain information constituting a commercial, state or other secret. The presence of technical channels for information leakage is due to physical processes associated with the propagation of acoustic, electromagnetic, and optical waves. Through such channels, leakage of acoustic, specific information, information processed by technical means and systems is possible. In the framework of this work, the features of certification of protected premises against leakage of acoustic information are considered. Certification includes instrumental measurements that allow you to detect an informative signal in communication lines, on the air, in heating, water supply, ventilation, etc. In addition to measurements, certification involves calculations based on which a conclusion is made about the conformity or non-compliance of the level of protection. The calculation part is rather cumbersome and complex, therefore the purpose of the work is to develop an algorithm that allows you to determine the degree of security of the selected premises from the leakage of speech information. The objectives of the work are: the development of auxiliary algorithms for calculating the security parameters of the room for each type of voice information leakage channel; implementation of software that allows you to determine the degree of security of the room; conducting a study of the dependence of room security on the noise level using the developed software. As the results of the work, the synthesized algorithm and the developed software tool should be noted, which can significantly reduce the time for the procedure for assessing the security of the room and avoid errors. The result of the work is the study of the dependence of verbal intelligibility of speech on the noise level in various octaves. Studies have shown that verbal intelligibility, which determines the security of a room by acoustic parameters, decreases non-linearly with an increase in the noise level at a fixed signal level.

Information security; speech information leakage; dedicated room; information leakage channel; premises security assessment.

Введение. На сегодняшний день вопросам защиты информации в организациях уделяется большое значение, потому что от этого существенно зависит конкурентоспособность коммерческих предприятий [1–7]. Для государственных учреждений это тем более актуально, т.к. их деятельность связана с обработкой большого количества персональных данных, а так же сведений, составляющих государственную тайну. Помещения, в которых производится обработка таких данных, нуждаются в специальном обследовании на предмет выявления возможных утечек информации по технических каналам [8–20]. К техническим каналам утечки информации относятся каналы утечки речевой информации [8–10].

Оценить актуальность угрозы утечки речевой информации можно по методикам, приведенным в [8–10]. В рамках оценки защищенности помещения предполагается два этапа: инструментальные измерения и расчетная часть, которая довольно объемна и требует значительных временных затрат.

Представляется актуальной разработка алгоритма и программного средства, реализующего оценку соответствия уровня защищенности помещения от утечек речевой информации требованиям нормативных документов по безопасности информации, поскольку это позволит существенно сократить временные затраты, а так же избежать ошибок в расчетах.

Алгоритм оценки защищенности помещения от утечек по техническим каналам. Перехватить речевую информацию можно по нескольким каналам, которые делятся на: акустические и вибрационные; каналы низкой частоты (НЧ); каналы высокой частоты (ВЧ); каналы утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Поэтому алгоритм оценки защищенности включает расчеты показателей по всем этим каналам (рис. 1). Более подробно рассмотрим работу алгоритма на примере оценки защищенности по акустическому и вибрационному каналам (рис. 2).

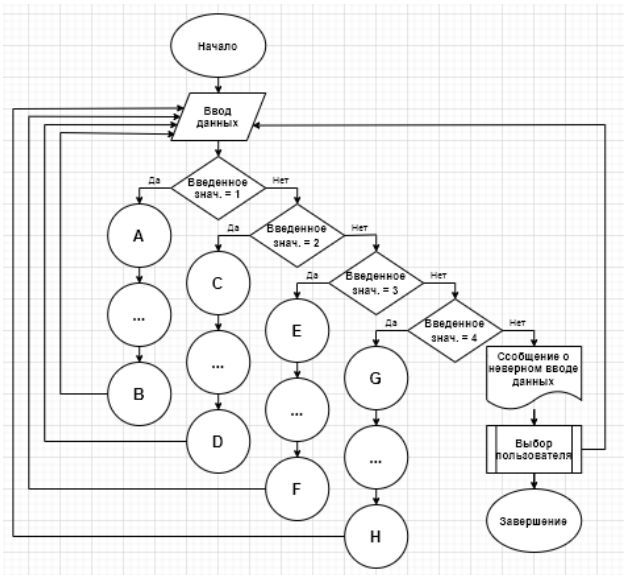

Рис. 1. Блок-схема основной программы

В данных каналах проводником утечки информации являются различные проемы и вентиляционные отверстия, ограждающие конструкции, трубы инженерных коммуникаций и т.д.

Показателем качества оценки защищенности помещения по данным каналам является словесная разборчивость речи *W*, под которой понимается процентное соотношение правильно понятых слов, зарегистрированных с использованием разведывательных средств.

Рис. 2. Блок-схема алгоритма оценки защищенности по акустическому и вибрационному каналам

Для расчета этого показателя может использоваться следующая методика [8, 9].

1) Расчет уровня звукового давления сигнала

$$L_{Ci} = 10\lg\left(10^{\frac{L_{C+Шi}}{10}} - 10^{\frac{L_{Шi}}{10}}\right), \quad (1)$$

где $L_{C+Шi}$ – уровень звукового давления аддитивной смеси сигнала и шума в *i*-й октавной полосе, дБ; $L_{Шi}$ – уровень звукового давления шума в *i* -й октавной полосе, дБ.

2) Расчет коэффициента превышения создаваемого звукового давления в каждой октаве над нормированным уровнем по следующей формуле:

$$\Delta_i = L_{Ci} - L_{Hi}, \quad (2)$$

L_{Hi} – нормированный уровень в *i*-й октавной полосе, дБ.

3) Расчет уровня сигнала, приведенного к нормированному уровню звукового давления в *i*-й октавной полосе

$$L_{C.прив.i} = L_{Ci} - \Delta_i. \quad (3)$$

4) Расчет соотношения сигнал-шум:

$$E_i = L_{C.прив.i} - L_{Шi}. \quad (4)$$

5) Расчет словесной разборчивости речи:

$$W_c = \begin{cases} 1.54 * R^{0.25} * \left(1 - e^{(-11*R)}\right), \text{ если } R < 0.15; \\ 1 - e^{\left(-\frac{11*R}{1+0.7*R}\right)}, \text{ если } R \geq 0.15, \end{cases} \quad (5)$$

где R – интегральный индекс артикуляции речи,

$$R = \sum_{i=1}^{N} (p_i * k_i), \quad (6)$$

k_i – весовой коэффициент каждой октавы.

Параметр p_i в выражении (6) вычисляется по следующей формуле:

$$p_i = \begin{cases} \frac{0.78 + 5.46 * e^{\left(-4.3*10^{-3}*\left(27.3-|Q_i|\right)^2\right)}}{1+10^{0.1*|Q_i|}}, \text{если } Q_i \leq 0; \\ 1 - \frac{0.78 + 5.46 * e^{\left(-4.3*10^{-3}*\left(27.3-|Q_i|\right)^2\right)}}{1+10^{0.1*|Q_i|}}, \text{если } Q_i > 0, \end{cases} \quad (7)$$

где Q_i определяется выражением

$$Q_i = E_i - \Delta A_i, \quad (8)$$

ΔA_i – значение форматного параметра речи в каждой октаве.

Описание программного средства. В рамках работы разработано программное средство, позволяющее определить степень защищенности выделенного помещения от утечки речевой информации. Далее проиллюстрирована часть программы, реализующая алгоритм оценки защищенности по акустическому и вибрационному каналам (рис. 3, 4).

Входные данные

	250	500	1000	2000	4000
TCi	88.15	100.69	89.13	87.98	88.24
C+Ши	48.86	45.23	41.45	52.26	58.22
Ши	25.78	25.12	22.05	22	25.49

Рис. 3. Входные данные, полученные в результате измерений

Источником входных данных (рис. 3) служат в результаты измерения. Для этого необходим шумомер, который измеряет уровень шумов за ограждающей конструкцией. К данному прибору подключается микрофон, для акустических измерений, и акселерометр – для вибрационных. Также важным элементом для измерения является акустический калибратор или эталон звукового давления. Для определения того, присутствует ли утечка информации, необходимо при помощи тестового сигнала измерить уровень звукового давления за пределами ограждающей конструкции. В качестве источника тест-сигнала используется генератор низкой частоты, подключенный к акустической колонке. Сигнал, прошедший через ограждающую конструкцию, значительно ослабляется относительно шумов. Результатом измерения является сумма сигнала и шума. При отключении акустической системы, проводятся измерения шумов за ограждающей конструкцией. На рис. 3 обозначению TCi соответствует уровень тесто-

вого сигнала в дБ, задаваемый для пяти октавных полос. Обозначению С+Ші соответствует уроню смеси сигнала и шума за ограждающей конструкцией ($L_{C+Ші}$). Ші – уровень шума за ограждающей конструкцией $L_{Ші}$.

На рис. 4 продемонстрирован результат вычислений.

Рис. 4. Выходные данные

Обозначениям Ci ,Hi, и С прив.i на рис. 4 соответствуют параметры L_{Ci} L_{Hi} и $L_{C.прив.i}$.

Значение словесной разборчивости составило 0,81, что превысило нормированные значения *W*пр.н = 0.3 и *W*непр.пр.н = 0.5 для преднамеренного и непреднамеренного прослушивания соответственно (рис. 4).

Исследование показателей защищенности выделенного помещения от утечки речевой информации. Для оценки защищенности от утечки речевой информации рассматривались каналы: акустические и вибрационные, НЧ, ВЧ и ПЭМИН [8–20].

В рамках эксперимента для улучшения наглядности результатов значение уровня шумов выбиралось одинаковым для каждой октавы. На рис. 5 приведена зависимость разборчивости речи от уровня шумов при оценке защищенности от возникновения акустических и вибрационных каналов.

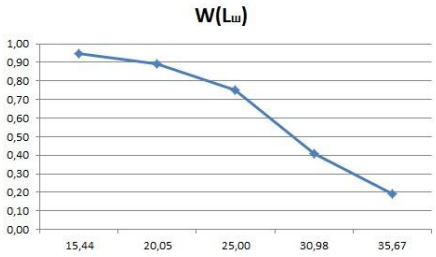

Рис. 5. График зависимости словесной разборчивости речи от уровня шумов за ограждающей конструкцией

Можно сделать вывод о том, что при увеличении уровня шумов за границей контролируемой зоны разборчивость речевой информации падает. Если она все же оказывается выше 0.3, то необходимо устанавливать определенные средства защиты информации или расширять границы контролируемой зоны.

Далее проводилось исследование защищенности выделенного помещения по НЧ-каналу. В ходе эксперимента изменялось значение напряжения шумов в линиях электропитания для того, чтобы определить зависимость относительно словесной разборчивости речи. Результаты эксперимента приведены на рис. 6. Исходя из рисунка 6, можно сделать вывод о том, что при увеличении зашумленности в ли-

ниях электропитания конфиденциальная информация, которой пытается завладеть злоумышленник, будет получена с явными искажениями при уровнях шумов свыше 43 дБ. В иных случаях необходимо также провести специальные организационные и технические меры по устранению возникшего канала.

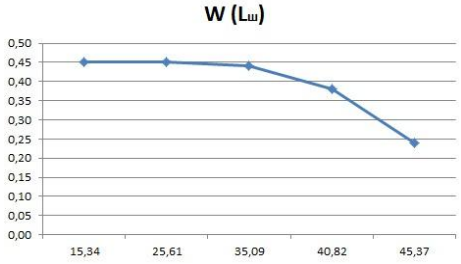

Рис. 6. График зависимости словесной разборчивости речи от уровня шумов в линиях электропитания

Аналогичные исследования были проведены для ВЧ-канала утечки информации. В рамках эксперимента исследовалась зависимость словесной разборчивости от уровня шумов в линиях электропитания. В отличие от НЧ канала утечки информации, в ВЧ навязывании злоумышленник подключается к линиям электропитания и может использовать следующие типы технических средств (ТС): стационарные, носимые и возимые. Следовательно, необходимо проводить исследования для всех ТС, чтобы дать корректную оценку защищенности выделенного помещения. Результаты исследований приведены на рис. 7–9. Видно, что наиболее опасными являются стационарные средства. Заданный уровень защищенности обеспечивается при уровне шумов более 38 дБ.

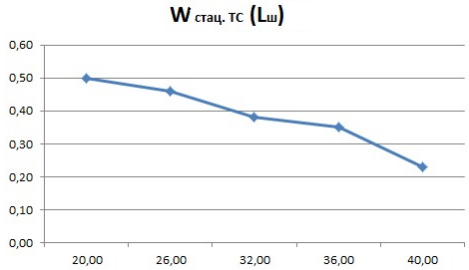

Рис. 7. График зависимости защищенности выделенного помещения от уровня шумов по ВЧ каналу с использованием стационарных ТС

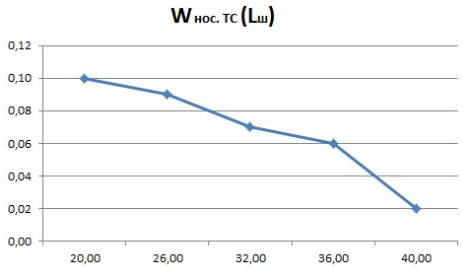

Рис. 8. График зависимости защищенности выделенного помещения от уровня шумов по ВЧ каналу с использованием носимых ТС

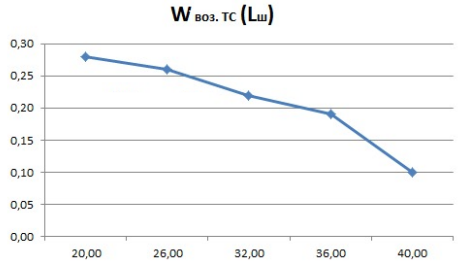

Рис. 9. График зависимости защищенности выделенного помещения от уровня шумов по ВЧ каналу с использованием возимых ТС

Далее рассмотрим результаты исследований канала утечки информации за счет ПЭМИН. Утечка информации через ПЭМИН возможна под воздействием информативных побочных излучений основных технических средств и систем за счет наводок, возникающих во вспомогательных технических средствах и системах. В качестве показателя для рассматриваемого канала утечки информации используется значение величины максимальной длины пробега цепи электропитания. На рис. 10 приведена зависимость данного параметра в метрах от уровня шумов.

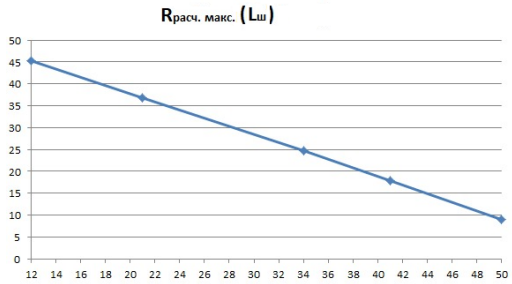

Рис. 9. График зависимости величины максимальной длины пробега исследуемой цепи электропитания от уровня шумов

Данный график позволят соотнести расчетную величину длины пробега исследуемой цепи с границами контролируемой зоны при заданном уровне шумов. Если эта длина превышает указанные границы, то в этом случае необходимо провести организационные и технические меры по устранению возможного канала утечки информации.

Заключение. В результате разработан и реализован в рамках программного средства алгоритм расчета степени защищенности выделенного помещения от утечки речевой информации. Приведен расчет защищенности от утечек по акустическим и вибрационным каналам. Проиллюстрирована работа программного средства, реализующего данный алгоритм.

Применение разработанного алгоритмического и программного обеспечения дает возможность существенно сократить время на процедуру оценки защищенности и избежать ошибок.

Так же проведено исследование показателей защищенности помещения с использованием разработанного программного средства, которое позволяет оценить зависимость защищенности помещения от уровня шумов.

В рамках эксперимента выявлено, что словесная разборчивость речи за ограждающей конструкцией опускается ниже критических значений при уровне шумов не менее 33,5 дБ.

При исследовании зависимости словесной разборчивости речи от уровня шумов в линиях электропитания для НЧ и ВЧ каналов получены минимальные значения уровней шумов (43 дБ и 38 дБ соответственно), при которых обеспечивается требуемая защищенность.

Исследование канала утечки информации через ПЭМИН показало, что чем меньше размеры контролируемой зоны, тем выше должен быть уровень шума. Так, например, при длине пробега исследуемой цепи электропитания меньше или равной 15 метрам уровень шума должен превышать 44 дБ, а при возможной длине пробега 30 метров уровень шума должен быть выше 29 дБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Баранова Е.К., Бабан А.В.* Информационная безопасность и защита информации: учеб. пособие. – 3-е изд. – М.: Изд-во Горячая линия-Телеком, 2016.
2. *Буковшин В.А., Болдырихин Н.В.* Современные проблемы информационной безопасности // Современные материалы, техника и технология: Сб. статей. – Курск, 2018. – С. 47-52.
3. *Буковшин В.А., Болдырихин Н.В.* Кибербезопасность как неотъемлемая часть информационного мира // Современные материалы, техника и технология: Сб. статей. – Курск, 2018. – С. 52-55.
4. *Прохорова О.В.* Информационная безопасность и защита информации. – Самара: **СГАСУ**, 2014.
5. *Меньшаков Ю.К.* Виды и средства иностранных технических разведок. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2009.
6. *Меньшаков Ю.К.* Основы защиты от технических разведок. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2011.
7. *Хорев А.А.* Организация контроля эффективности противодействия техническим средствам разведки и защиты информации. – М.: МО РФ, 2006.
8. *Бузов Г.А., Калинин С.В., Кондратьев А.В.* Защита от утечки информации по техническим каналам. – М.: Горячая линия-Телеком, 2005.
9. *Дураковский А.П., Куницын И.В., Лаврухин Ю.Н.* Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации. – М.: НИЯУ МИФИ, 2015. – 152 с.
10. *Железняк В.К., Макаров Ю.К., Хореев А.А.* Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – 2000. – № 4. – С. 39-45.
11. *Гончаров Р.А., Короченцев Д.А., Зеленский А.А.* Разработка подсистемы поддержки принятия решения идентификации технических каналов утечки информации // Национальная Ассоциация Ученых. – 2018. – № 14 (41). – С. 8-11.
12. *Голуб Б.В., Максимов Р.В.* Технические средства и методы защиты информации от утечки по техническим каналам // Хроники объединенного фонда электронных ресурсов «Наука и образование». – М.: Институт управления образованием Российской академии образования, 2014.
13. *Давыдов А.Е., Максимов Р.В., Савицкий О.К.* Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации. – СПб.: НИИ "Масштаб", 2012.
14. *Евстифеев А.А., Ерошев В.И., Казаков А.А.* Разработка предложений по оценке защищенности информации технических систем от утечки по техническим каналам // Математика и математическое моделирование: Сб. статей. – Саров, 2018. – С. 15-16.
15. *Зеленский А.А., Короченцев Д.А., Ревякина Е.А.* Разработка адаптивного fuzzy-алгоритма идентификации технических каналов утечки информации // Colloquium-journal. – 2020. – № 11-1 (63). – С. 40-44.
16. *Короченцев Д.А., Зеленский А.А.* Система идентификации технических каналов утечки информации // Актуальные проблемы науки и техники: Сб. тезисов докладов. – Ростов-на-Дону, 2019. – С. 357-358.
17. *Лукьянов А.С., Перминов Г.В*. Разновидности и особенности технических каналов утечки информации // Охрана, безопасность, связь: Сб. статей. – Воронеж: 2013. – С. 41-44.

18. *Садовская Т.Г., Хорев А.А.* Средства и методы обеспечения безопасности бизнеса. Технические каналы утечки информации. – М.: МГТУ им. Н.Э. Баумана, 2009.
19. *Тегенцев И.М., Щербаков В.А., Пономаренко С.А.* Формализация процессов комплексного технического контроля защищенности информации от утечки по техническим каналам // Охрана, безопасность, связь: Сб. статей. – Воронеж, 2016. – № 1-2. – С. 150-154.
20. *Торокин А.А.* Инженерно-техническая защита информации. – М.: МО РФ, 2004.

REFERENCES

1. *Baranova E.K., Baban A.V.* Informatsionnaya bezopasnost' i zashchita informatsii: ucheb. Posobie [Information security and information protection: studies. Stipend]. 3rd ed. Moscow: Izd-vo Goryachaya liniya-Telekom, 2016.
2. *Bukovshin V.A., Boldyrikhin N.V.* Sovremennye problemy informatsionnoy bezopasnosti [Modern problems of information security], *Sovremennye materialy, tekhnika i tekhnologiya: Sb. statey* [Modern materials, technique and technology: Collection of articles]. Kursk, 2018, pp. 47-52.
3. *Bukovshin V.A., Boldyrikhin N.V.* Kiberbezopasnost' kak neot"emlemaya chast' informatsionnogo mira [Cybersecurity as an integral part of the information world], *Sovremennye materialy, tekhnika i tekhnologiya: Sb. statey* [Modern materials, technique and technology: Collection of articles]. Kursk, 2018, pp. 52-55.
4. *Prokhorova O.V.* Informatsionnaya bezopasnost' i zashchita informatsii [Information security and information protection]. Samara: SGASU, 2014.
5. *Men'shakov Yu.K.* Vidy i sredstva inostrannykh tekhnicheskikh razvedok [Types and means of foreign technical intelligence]. Moscow: Izd-vo MGTU im. N.E. Baumana, 2009.
6. *Men'shakov Yu.K.* Osnovy zashchity ot tekhnicheskikh razvedok [Fundamentals of protection from technical intelligence]. Moscow: Izd-vo MGTU im. N.E. Baumana, 2011.
7. *Khorev A.A.* Organizatsiya kontrolya effektivnosti protivodeystviya tekhnicheskim sredstvam razvedki i zashchity informatsii [Organization of control over the effectiveness of counteraction to technical means of intelligence and information protection]. Moscow: MO RF, 2006.
8. *Buzov G.A., Kalinin S.V., Kondrat'ev A.V.* Zashchita ot utechki informatsii po tekhnicheskim kanalam [Protection against information leakage through technical channels]. Moscow: Goryachaya liniya-Telekom, 2005.
9. *Durakovskiy A.P., Kunitsyn I.V., Lavrukhin Yu.N*. Kontrol' zashchishchennosti rechevoy informatsii v pomeshcheniyakh. Attestatsionnye ispytaniya vspomogatel'nykh tekhnicheskikh sredstv i sistem po trebovaniyam bezopasnosti informatsii [Monitoring the security of speech information in the premises. Attestation tests of auxiliary technical means and systems for information security requirements]. Moscow: NIYAU MIFI, 2015, 152 p.
10. *Zheleznyak V.K., Makarov Yu.K., Khoreev A.A.* Nekotorye metodicheskie podkhody k otsenke effektivnosti zashchity rechevoy informatsii [Some methodological approaches to evaluating the effectiveness of speech information protection], *Spetsial'naya tekhnika* [Special technique], 2000, No. 4, pp. 39-45.
11. *Goncharov R.A., Korochentsev D.A., Zelenskiy A.A*. Razrabotka podsistemy podderzhki prinyatiya resheniya identifikatsii tekhnicheskikh kanalov utechki informatsii [Development of a decision support subsystem for identifying technical channels of information leakage], *Natsional'naya Assotsiatsiya Uchenykh* [National Association of Scientists], 2018, No. 14 (41), pp. 8-11.
12. *Golub B.V., Maksimov R.V.* Tekhnicheskie sredstva i metody zashchity informatsii ot utechki po tekhnicheskim kanalam [Technical means and methods of protecting information from leaks through technical channels], *Khroniki ob"edinennogo fonda elektronnykh resursov «Nauka i obrazovanie»* [Chronicles of the United Fund of electronic resources "Science and education"]. Moscow: Institut upravleniya obrazovaniem Rossiyskoy akademii obrazovaniya, 2014.
13. *Davydov A.E., Maksimov R.V., Savitskiy O.K.* Tekhnicheskie sredstva i metody zashchity informatsii ot utechki po tekhnicheskim kanalam na ob"ektakh informatizatsii [Technical means and methods of information protection from leakage through technical channels to the information objects]. Saint Petersburg: NII "Masshtab", 2012.
14. *Evstifeev A.A., Eroshev V.I., Kazakov A.A.* Razrabotka predlozheniy po otsenke zashchishchennosti informatsii tekhnicheskikh sistem ot utechki po tekhnicheskim kanalam [Development of proposals for assessing the security of information from technical systems leakage through technical channels], *Matematika i matematicheskoe modelirovanie: Sb. statey* [Mathematics and mathematical modeling: a Collection of articles]. Sarov, 2018, pp. 15-16.

15. *Zelenskiy A.A., Korochentsev D.A., Revyakina E.A.* Razrabotka adaptivnogo fuzzy-algoritma identifikatsii tekhnicheskikh kanalov utechki informatsii [Development of an adaptive fuzzy algorithm for identifying technical channels of information leakage], *Colloquium-journal* [Colloquium-journal], 2020, No. 11-1 (63), pp. 40-44.
16. *Korochentsev D.A., Zelenskiy A.A.* Sistema identifikatsii tekhnicheskikh kanalov utechki informatsii [Identification system for technical channels of information leakage], *Aktual'nye problemy nauki i tekhniki: Sb. tezisov dokladov* [Actual problems of science and technology: Collection of abstracts]. Rostov-on-Don, 2019, pp. 357-358.
17. *Luk'yanov A.S., Perminov G.V.* Raznovidnosti i osobennosti tekhnicheskikh kanalov utechki informatsii [Varieties and features of technical channels of information leakage], *Okhrana, bezopasnost', svyaz': Sb. statey* [Security, safety, communication: Collection of articles]. Voronezh: 2013, pp. 41-44.
18. *Sadovskaya T.G., Khorev A.A.* Sredstva i metody obespecheniya bezopasnosti biznesa. Tekhnicheskie kanaly utechki informatsii [Tools and methods for ensuring business security. Technical channels of information leakage]. Moscow: MGTU im. N.E. Baumana, 2009.
19. *Tegentsev I.M., Shcherbakov V.A., Ponomarenko S.A.* Formalizatsiya protsessov kompleksnogo tekhnicheskogo kontrolya zashchishchennosti informatsii ot utechki po tekhnicheskim kanalam [Formalization of processes of complex technical control of information security from leakage through technical channels], *Okhrana, bezopasnost', svyaz': Sb. statey* [Security, safety, communication: Collection of articles]. Voronezh, 2016, No. 1-2, pp. 150-154.
20. *Torokin A.A.* Inzhenerno-tekhnicheskaya zashchita informatsii [Engineering and technical protection of information]. Moscow: MO RF, 2004.

Статью рекомендовал к опубликованию д.т.н. В.А. Погорелов.

Чуб Павел Андреевич – Донской государственный технический университет; e-mail: pavel.chub.1997@mail.ru; 344000, г. Ростов-на-Дону, ул. Мечникова, 154А, кв. 810; тел.: +79185140041; кафедра кибербезопасности информационных систем; студент.

Цветкова Диана Николаевна – e-mail: tswetckowa.diana@yandex.ru; 344018, г. Ростов-на-Дону, ул. Юфимцева, 14/2, кв. 60; тел.: +79198976476; кафедра кибербезопасности информационных систем; студентка.

Болдырихин Николай Вячеславович – e-mail: boldyrikhin@mail.ru; 344065, г. Ростов-на-Дону, пер. Днепровский, 116К, кв. 111; тел.: +79043442295; кафедра кибербезопасности информационных систем; к.т.н.; доцент.

Короченцев Денис Александрович – e-mail: mytelefon@mail.ru; 344038, г. Ростов-на-Дону, пр. Михаила Нагибина, 29, кв. 24; тел.: +7903489173; кафедра кибербезопасности информационных систем; зав. кафедрой; к.т.н.

Chub Pavel Andreyevich – Don State Technical University; e-mail: pavel.chub.1997@mail.ru; 154A, Mechnikova street, apt. 810, Rostov-on-Don, 344000, Russia; phone: +79185140041; the department of cybersecurity of information systems; student.

Tsvetkova Diana Nikolaevna – e-mail: tswetckowa.diana@yandex.ru; 14/2, Yufimtseva street, apt. 60, Rostov-on-Don, 344018, Russia; phone: +79198976476; the department of cybersecurity of information systems; student.

Boldyrikhin Nikolay Vyacheslavovich – e-mail: boldyrikhin@mail.ru; 116K, per. Dneprovsky, apt. 111, Rostov-on-Don, 344065, Russia; phone: +79043442295; the department of cybersecurity of information systems; cand. of eng. sc.; associate professor.

Korochentsev Denis Aleksandrovich – e-mail: mytelefon@mail.ru; 29, Mikhail Nagibin Ave., apt. 24, Rostov-on-Don, 344038, Russia; phone: +79034895173; the department of cybersecurity of information systems; cand. of eng. sc.; head of the department.