Для цитирования: Рогозин Е.А., Силка Д.Г., Гуляев О.А. Методика оценивания защищенности информации по техническим каналам на объекте информатизации специального назначения. Вестник Дагестанского государственного технического университета. Технические науки. 2019; 46 (4): 123-133. DOI:10.21822/2073-6185-2019-46-4-123-133

For citation: E.A. Rogozin, D.G. Silka, O.A. Gulyaev. Methodology for assessing the security of information passed through the technical channels of a special-purpose informatisation object. Herald of Daghestan State Technical University. Technical Sciences. 2019; 46 (4): 123-133. (in Russ.) DOI:10.21822/2073-6185-2019-46-4-123-133

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.3: 004.05

DOI: 10.21822/2073-6185-2019-46-4-123-133

МЕТОДИКА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Рогозин Е.А.¹, Силка Д.Г.¹, Гуляев О.А.²

¹ Воронежский институт Министерства внутренних дел России,

¹394065, г. Воронеж, пр. Патриотов, 53, Россия,

²АО «Аэроприбор Восход»,

²105318, г. Москва, ул. Ткацкая, д. 19, Россия

Резюме: Цель. В целях определения «защищенности» объекта информатизации специального назначения, необходимо провести расчёт показателей эффективности мероприятий по защите информации (ЗИ) от угроз НСД, связанных с утечкой информации по техническим каналам (по акустическому каналу). С целью определения актуальных каналов утечки информации необходимо разработать перечень действий, по нейтрализации потенциальных угроз (включая разработку системы защиты информации для объекта информатизации специального назначения). **Метод.** Оценка защищенности объекта информатизации специального назначения проводится с использованием экспертно-документального и инструментального методов. **Результат.** Приведены результаты оценивания показателей защищённости от утечки информации по воздушному (акустическому) каналу и определены аспекты совершенствования специальных мероприятий по защите информации на объекте информатизации специального назначения. **Вывод.** Направление данного исследования является весьма актуальным и требует дальнейшего развития организационно-технических мероприятий, по реализации требований нормативно правовых документов по защите информации на объектах информатизации специального назначения.

Ключевые слова: объект информатизации специального назначения, оценка защищенности, аттестационные испытания, эффективность, утечка защищаемой информации, несанкционированное получение информации, закладные устройства

METHODOLOGY FOR ASSESSING THE SECURITY OF INFORMATION PASSED THROUGH THE TECHNICAL CHANNELS OF A SPECIAL-PURPOSE INFORMATISATION OBJECT

E.A. Rogozin¹, D.G. Silka¹, O.A Gulyaev²

*Voronezh Institute of the Ministry of the Interior of the Russian Federation,
53 Patriotov St., Voronezh 394065, Russia,*

²Joint Stock Company «Aeroprivor Voskhod»,

²19 Tkatskaya St., Moscow 105318, Russia

Abstract Objectives. In order to determine the security of a special-purpose informatisation object, it is necessary to calculate the effectiveness indicators of information security (IS) measures aimed at preventing unauthorised access (UA) threats associated with information leakage through technical (acoustic) channels. In order to determine the actual channels of information leakage, it is necessary to develop a list of actions to neutralise potential threats, including the development of an information protection system for a special-purpose informatisation object. **Method.** A security assessment of the special-purpose informatisation object is carried out using expert documentary and instrumental methods. **Results.** The results of evaluating the indicators of protection against information leakage through the air (acoustic) channel are presented and aspects of improving special measures for protecting information at the special-purpose informatisation object are identified. **Conclusion.** Due to its relevance, the direction of this study requires further development of organisational and technical measures to implement the requirements of regulatory documents on the protection of information in special-purpose informatisation objects.

Keywords: special purpose informatisation object, security assessment, certification tests, efficiency, leakage of protected information, unauthorised access, covert devices

ведение. Для выполнения поставленной задачи необходимо изучить исходные данные рассматриваемого объекта информатизации специального назначения. В качестве примера был рассмотрен потенциальный объект информатизации, в котором могут проходить конфиденциальные совещания, план которого изображен на (рис.1).

Рис. 1. Размещение объекта информатизации специального назначения относительно границ КЗ
Fig. 1. Placement of a special-purpose informatization object relative to the boundaries of the short circuit

В дальнейшем этот кабинет будем трактовать и интерпретировать, как объект информатизации специального назначения (ОИЧН).

На ОИЧН находятся следующие технические средства представленные табл.1.

Таблица 1. Технические средства
Table 1. Technical means

№	Название Name	Тип, модель Type, Model	Заводской номер Serial Number	Класс Class TC
1	Акустический модуль Acoustic module	ОП 073	ТЗИ001387	BTCC
2	Видеодвойка Video double	Samsung DVD-V8500K	6VCY902678Z	BTCC
3	Видеопроектор Video projector	Sanyo PLC-XV70	№66410747	OTCC
4	Ноутбук Laptop	Acer Aspire 4702Z	№LXAL70X00274305892	OTCC
5	Датчик пожарной сигнализации (2шт.) Fire Alarm Sensor (2pcs.)	Bolid ДИП-34А	ТЗИ 001389ТЗИ 001388	BTCC
6	Колонка акустическая Acoustic speaker	Inter M SWS-03	020216407 Л2827839	BTCC
7	Розетка электрическая Sockets	Рондо Sch. E RS16 - 121	ТЗИ 001380	BTCC
8	Акустическая система Speaker System (5 + 1) (5+1)	BBK MA-900S	АО0550514832 Л2827834	OTCC
Л1	Линия для акустического модуля ОП 073 Line for acoustic module OP 073	Двухжильный медный провод Two-core copper wire	-	-
Л2	Линия электропитания Power line	Двухжильный медный провод Two-core copper wire	-	-
Л3	Линия для оповещения посредством Inter M SWS-03 Alert line via Inter M SWS-03	Двухжильный медный провод Two-core copper wire	-	-
Л4	Линия пожарной сигнализации Fire alarm line	Двухжильный медный провод Two-core copper wire	-	-

Постановка задачи. Исходя из визуального анализа каналов утечки информации, можно сделать вывод, что на ОИСН возможна утечка информации по следующим техническим каналам: 1. по воздушному (акустическому) каналу; 2. по вибрационному каналу; 3. по параметрическому каналу; 4. по оптико-электронному каналу; 5. по электроакустическому каналу [4,5].

Кроме того, так как при проведении совещаний широко используются бумажные носители защищаемой информации, средства визуального отображения информации (монитор ПК и видеопроектор), необходимо так же рассматривать и визуальный канал утечки информации.

Таким образом, необходимо провести оценивание реальной защищенности для ОИСН от утечки информации по следующим техническим каналам: визуальному каналу; воздушному (акустическому) каналу; виброакустическому каналу; электроакустическому каналу; оптико-электронному каналу; параметрическому каналу.

Оценивание защищенности ОИСН от утечки информации по техническим каналам является составной частью мероприятий при аттестации объектов информатизации по требованиям безопасности информации, которая, в свою очередь, призвана подтвердить, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Методы исследования. Для оценивания защищенности ОИСН от утечки защищаемой информации по воздушному (акустическому) каналу применялся как экспертно-документальный, так и инструментальный метод [1,3,5].

Утечка речевой информации по воздушному (акустическому) каналу возможна:

1. Через закладные устройства, установленные в ограждающих конструкциях или предметах интерьера.
2. Через закладные устройства, вмонтированные во вспомогательные технические средства.
3. Через ограждающие конструкции (двери, стены, воздуховоды, окна) путем прямого прослушивания, вследствие недостаточной звукоизоляции.

Разберем последовательно каждую возможность.

1. Однозначно говорить об отсутствии закладочных устройств, установленных в ограждающих конструкциях или предметах интерьера можно только после проведения комплекса мероприятий по поиску данных устройств – специального обследования объекта информатизации специального назначения. Результаты специального обследования оформляются актом. При изучении документации на данное помещение акт специального обследования обнаружен не был, сведения о проведении данного мероприятия отсутствуют. Следовательно, существует вероятность утечки защищаемой информации через закладные устройства, установленные в ограждающих конструкциях или предметах интерьера.

2. Специальная проверка вспомогательных технических средств проводится только для средств иностранного производства. На объекте информатизации специального назначения находятся вспомогательные технические средства (ВТСС) в составе: системы звукоусиления ВВК МА-900S, динамиков системы оповещения Inter M SWS-03 и ОП 073, видеодвойки Samsung DVD-V8500K и датчиков пожарной сигнализации Bolid ДИП-34А. Динамики системы оповещения и датчики пожарной сигнализации отечественного производства, следовательно, не подлежат обязательной специальной проверке, тем не менее, с большой вероятностью компоненты из которых состоят устройства, произведены за рубежом, поэтому специальную проверку устройства должны пройти. Система звукоусиления и видеодвойка специальную проверку проходили, об этом свидетельствуют соответствующие акты.

3. Для оценивания защищенности объекта информатизации специального назначения от утечки информации путем прямого прослушивания через ограждающие конструкции применялся комплекс «Спрут-11М». Проверка выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу заключается в количественной оценке величины показателя эффективности защиты речевой информации с последующим ее сравнении с нормированными значениями [1,2].

Эффективность защиты речевой информации от утечки по акустическому каналу оценивается по одному из двух показателей: словесная разборчивость речи, определяемая в контрольных точках; распределение отношений «речевой сигнал/акустический шум» в октавных полосах частот в контрольных точках.

Контрольными точками (КТ) являются места возможной установки акустических и вибрационных датчиков аппаратуры акустической речевой разведки, или места расположения отражающих поверхностей, уязвимых для лазерного съема речевой информации (в первую очередь это оконные стекла), а также места непреднамеренного прослушивания речи, в которых производится измерение отношений «сигнал/шум».

При выборе контрольных точек необходимо строго следовать рекомендациям, изложенным в нормативно-методических документах по контролю эффективности защиты информации от акустической речевой разведки [1,5]. Возможные варианты утечки речевой информации из объекта информатизации представлены на рис.2.

Рис. 2. Утечка речевой информации из помещения
Fig. 2. Leak of speech information from the premises

В процессе аттестационных испытаний измерительный микрофон располагается на средней вертикальной линии на расстоянии от 1 до 2 метров от измеряемой ограждающей конструкции или ее участка.

Защищенность речевой информации от ее перехвата по электронно-оптическому каналу аппаратурой технической разведки считается обеспеченной, если значение контролируемого параметра, рассчитанного по результатам измерений на оконном остеклении, не превышает нормированного значения.

Контрольные точки выбираются на расстоянии 0,5 м от ограждающих конструкций на высоте 1,5 м от пола с внешней стороны объекта информатизации.

Контрольные точки изображены на рис.3, рис.4, рис.5, рис.6.

Рис. 3. Контрольные точки на стенах
Fig. 3. Control points on the walls

Рис. 4. Контрольные точки между этажами
Fig. 4. Control points between floors

Рис. 5. Контрольные точки на трубах отопления
Fig. 5. Test points on heating pipes

Рис. 6. Контрольные точки на окнах
Fig. 6. Control points on the Windows

Выберем контрольные точки на внешних поверхностях ограждающих конструкций:

- Контрольная точка 1.1 – дверь ОИЧН;
- Контрольная точка 1.2 – стена смежного помещения;
- Контрольная точка 1.3 – помещение на нижнем этаже;
- Контрольная точка 1.4 – помещение на нижнем этаже;
- Контрольная точка 2.1 – батарея отопления, выходящая в смежное помещение;
- Контрольная точка 2.2 – Контрольная точка 2.5 – батареи отопления, выходящие на нижний этаж;
- Контрольная точка 3.1 – Контрольная точка 3.24 – окна в ОИЧН;

В связи с тем, что окна выходят на проезжую часть, существует прямая угроза для защищаемой информации, следовательно, установка акустических датчиков аппаратуры акустической речевой разведки должна быть произведена.

В результате инструментального контроля с использованием комплекса «Спрут-11М» получены данные по акустическому сигналу для помещения.

Обсуждение результатов. Ниже представлены расчеты выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу для первой контрольной точки 1.1. (табл. 2).

Контрольная точка 1.1 – дверь ОИЧН на расстоянии 0,5 м от внешней поверхности двери.

Таблица 2. Результаты измерений в октавных полосах, в контрольной точке 1.1

Table 2. Measurement results in octave bands, at control point 1.1

Номер октавной полосы, i Octave band number	Среднегеометрическая частота октавной полосы, Гц The geometric mean frequency of the octave band, Hz	Уровень акустического шума в контрольной точке $L_{ш_i}$, дБ The level of acoustic noise at the control point $L_{ш_i}$, dB	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L_{(c+ш)_i}$, дБ The level of the total acoustic signal and acoustic noise at the control point $L_{(c+w)_i}$, dB
1	125	52,26	53,83
2	250	65,23	65,38
3	500	60,18	60,48
4	1000	57,50	57,89
5	2000	56,42	58,03
6	4000	61,43	61,76
7	8000	55,94	56,15

Расчеты по остальным контрольным точкам производились аналогичным образом. Данные по результатам расчетов приведены в табл. 3-5.

1. Вычисляем уровень акустического сигнала в контрольной точке 1.1 для семи октавных полос по следующей формуле:

$$L_{C_i} = 10 \lg \{ 10^{0,1L_{(c+ш)_i}} - 10^{0,1L_{ш_i}} \}$$

$$L_{C_1} = 10 \lg \{ 10^{0,1 \cdot 53,83} - 10^{0,1 \cdot 52,26} \} = 48,65$$

$$L_{C_2} = 10 \lg \{ 10^{0,1 \cdot 65,38} - 10^{0,1 \cdot 65,23} \} = 50,68$$

$$L_3 = 10 \lg \{ 10^{0,1 \cdot 60,48} - 10^{0,1 \cdot 60,18} \} = 48,72$$

$$L_{C_4} = 10 \lg \{ 10^{0,1 \cdot 57,89} - 10^{0,1 \cdot 57,50} \} = 47,22$$

$$L_{C_5} = 10 \lg \{ 10^{0,1 \cdot 58,03} - 10^{0,1 \cdot 56,42} \} = 52,94$$

$$L_{C_6} = 10 \lg \{ 10^{0,1 \cdot 61,76} - 10^{0,1 \cdot 61,43} \} = 50,40$$

$$L_{C_7} = 10 \lg \{ 10^{0,1 \cdot 56,15} - 10^{0,1 \cdot 55,94} \} = 42,89$$

2. Рассчитываются отношения сигнал/шум в октавных полосах.

В случае акустического сигнала:

$$E_i = L_{C_i} - L_{ш_i}$$

$$E_1 = L_{C_1} - L_{ш_1} = 48,64 - 52,26 = -5,18$$

$$E_2 = L_{C_2} - L_{ш_2} = 50,48 - 65,23 = -14,69$$

$$E_3 = L_{C_3} - L_{ш_3} = 48,65 - 60,18 = -11,75$$

$$E_4 = L_{C_4} - L_{ш_4} = 47,27 - 57,50 = -10,66$$

$$E_5 = L_{C_5} - L_{ш_5} = 52,96 - 56,42 = -5,09$$

$$E_6 = L_{C_6} - L_{ш_6} = 50,40 - 61,43 = -11,35$$

$$E_7 = L_{C_7} - L_{ш_7} = 42,88 - 55,94 = -13,26$$

Полученный результат E_i сравнивается с нормированным значением отношения «сигнал/шум» в октавных полосах $E_{н_i}$, приведенными в табл.2 НМД АРР.

После сравнения E_i с нормированными значениями можно сделать вывод, что нормы противодействия не выполняются. Так как условие $E_i \leq E_{н_i}$ не выполняется хотя ни для одной октавы, вычисляются октавные индексы артикуляции речи:

$$r_i = K_i \left| z - \frac{0,78 + 5,46 \exp[-4,3 \cdot 10^{-3} (27,3 - |E_i - A_i|)^2]}{1 + 10^{0,1|E_i - A_i|}} \right|$$

$$\text{где } z = \begin{cases} 0, & \text{если } E_i \leq A_i \\ 1, & \text{если } E_i > A_i \end{cases}$$

A_i – формантный параметр спектра речевого сигнала в октавной полосе, дБ;

K_i – весовой коэффициент октавной полосы частот.

Таблица 3. Числовые значения формантного параметра спектра речевого сигнала D Ai и весового коэффициента Ki в октавных полосах

Table 3. Numerical values of the formant parameter of the spectrum of the speech signal D Ai and the weight coefficient Ki in octave bands

Наименование параметров Name of parameters	Среднегеометрические частоты октавных полос fcp.i, Гц Geometrical mean frequencies of octave bands fcp.i, Hz						
	125	250	500	1000	2000	4000	8000
Числовое значение формантного параметра спектра речевого сигнала в октавной полосе D Ai, дБ The numerical value of the formant parameter of the spectrum of the speech signal in the octave band D Ai, dB	25	18	14	9	6	5	4
Числовое значение весового коэффициента в октавной полосе Ki The numerical value of the weight coefficient in the octave band Ki	0,01	0,03	0,12	0,2	0,3	0,26	0,07

Вычисляются октавные индексы артикуляции речи:

$$r_1 = 0,01 \left| 0 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-3,62 - 25|)^2]}{1 + 10^{0,1|-3,62-25|}} \right|$$

$$r_1 = 0,00003$$

$$r_2 = 0,03 \left| 0 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-14,75 - 18|)^2]}{1 + 10^{0,1|-14,75-18|}} \right|$$

$$r_2 = 0,02999$$

$$r_3 = 0,12 \left| 1 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-11,53 - 14|)^2]}{1 + 10^{0,1|-11,53-14|}} \right|$$

$$r_3 = 0,11845$$

$$r_4 = 0,2 \left| 1 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-10,23 - 9|)^2]}{1 + 10^{0,1|-10,23-9|}} \right|$$

$$r_4 = 0,19587$$

$$r_5 = 0,03 \left| 1 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-3,46 - 6|)^2]}{1 + 10^{0,1|-3,46-6|}} \right|$$

$$r_5 = 0,27912$$

$$r_6 = 0,26 \left| 1 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-11,03 - 5|)^2]}{1 + 10^{0,1|-11,03-5|}} \right|$$

$$r_6 = 0,25541$$

$$r_7 = 0,07 \left| 1 - \frac{0,78 + 5,46 \exp[-4,3 * 10^{-3} (27,3 - |-13,06 - 4|)^2]}{1 + 10^{0,1|-13,06-4|}} \right|$$

$$r_7 = 0,06919$$

3. Рассчитывается интегральный индекс артикуляции речи:

$$R = \sum_{i=1}^5 r_i = 0,00003 + 0,02999 + 0,11845 + 0,19587 + 0,27912 + 0,25541 + 0,06919$$

$$= 0,94807$$

4. Рассчитывается значение показателя противодействия APP:

$$W = \begin{cases} 1,54R^{0,25}[1 - \exp(-11R)], & \text{если } R < 0,15 \\ 1 - \exp\left(-\frac{11R}{1 + 0,7R}\right), & \text{если } R \geq 0,15 \end{cases}$$

Так как $R \geq 0,15$ ($0,94807 \geq 0,15$), то значение показателя противодействия APP рассчитываю по формуле:

$$W = 1 - \exp\left(-\frac{11R}{1 + 0,7R}\right)$$

$$W = 1 - \exp\left(-\frac{11 * 0,7587}{1 + 0,7 * 0,7587}\right) = 0,998$$

Сравнив полученные в результате расчетов контрольных точек, значения показателя противодействия APP с нормированными, можно сделать вывод, что нормы не выполняются и утечка защищаемой информации возможна.

Таблица 4. Результаты показателя противодействия W по каждой из контрольных точек
Table 4. The results of the counteraction index W for each of the control points

Контрольные точки	Значение показателя противодействия W
1.1	0,998
1.2	0,984
1.3	0,911
1.4	0,863
2.1	0,932
2.2	0,933
2.3	0,992
2.4	0,845
2.5	0,654
3.1	0,922
3.2	0,885
3.3	0,931
3.4	0,936
3.5	0,988
3.6	0,943
3.7	0,954
3.8	0,978
3.9	0,922
3.10	0,935
3.11	0,993
2.12	0,954
3.13	0,995
3.14	0,934
3.15	0,911
3.16	0,945
3.17	0,966
3.18	0,987
3.19	0,945
3.20	0,957
3.21	0,924
3.22	0,876
3.23	0,968
3.24	0,890

Таблица 5. Результаты определения отношений «сигнал/шум» в октавных полосах в контрольной точке KT1.1.

Table 5. The results of determining the signal-to-noise ratios in octave bands at the control point KT1.1.

Номер октавной полосы, i Octave band number	Уровень акустического шума в контрольной точке $L_{шi}$, дБ Acoustic noise level at the control point, $L_{шi}$, dB	Уровень суммарного акустического сигнала и акустического шума в контрольной точке $L(c+ш)i$, дБ The level of the total acoustic signal and acoustic noise at the control point $L(s+w)i$, dB	Уровень акустического сигнала в контрольной точке L_{ci} , дБ Acoustic signal level at the control point L_{ci} , dB	Отношение сигнал/шум в контрольной точке Ei , дБ Signal to Noise Ratio at Checkpoint Ei , dB
1	52,26	53,83	48,65	-5
2	65,23	65,38	50,68	-14
3	60,18	60,48	48,72	-11
4	57,50	57,89	47,22	-10
5	56,42	58,03	52,94	-5
6	61,43	61,76	50,40	-11
7	55,94	56,15	42,89	-13

Вывод. Таким образом, анализ результатов оценивания защищенности позволяет сделать следующий вывод, что существует реальная возможность утечки речевой информации через ограждающие конструкции, а также несанкционированное получения информации с помощью закладных устройств, установленных в ВТСС или ограждающих конструкциях. Для защиты объекта информатизации специального назначения подтверждена необходимость использования средств активной защиты информации от утечки по акустическому и виброакустическому каналам, что позволит реально повысить защищенности ОИЧН.

Библиографический список:

1. Зайцев А.П., Шелупанов А.А., Технические средства и методы защиты информации. М.: Машиностроение, 2009. – 507 с.
2. Хорев А.А., Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия РФ, 1998. – 320 с.
3. Кабанов А.С. Временная модель оценивания риска нарушения информационной безопасности / А.С. Кабанов, А.Б. Лось, В.И. Трунцев // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. Т. 1. № 25. С. 87-91.
4. Хорев А.А., Способы и средства защиты информации. Учебное пособие. – М.: МО РФ, 2000. – 316 с.
5. Торокин А.А.. Инженерно-техническая защита информации: Гелиос АРВ. – 2005, - 960с.
6. Бузов Г.А. Защита от утечки информации по техническим каналам : учеб. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. М.: Горячая линия Телеком, 2014. 416 с.
7. Charaf H. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. pp. 277–282.
8. Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Sliwa // Entropy. 2014. Vol. 16. Issue 12. pp. 6602–6623.
9. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). — 2016. pp. 133–187.
10. Павловский Ю.Н. Имитационные модели и системы / Ю.Н. Павловский. — М.: Фазис: ВЦ РАН, 2000. С. 134.
11. Краснощёков П.С. Оптимизация в автоматизированном проектировании / П.С. Краснощёков, В.В. Морозов, Н.М. Попов. М.: МАКС Пресс, 2008. 323 с.
12. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. pp. 1–5.
13. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114–118.
14. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. Vol. 94. pp. 1–24.

References:

1. Zaytsev A.P., Shelupanov A.A., Tekhnicheskiye sredstva i metody zashchity informatsii. M.: Mashinostroyeniye, 2009. – 507 s. [Zaitsev AP, Shelupanov AA, Technical means and methods of information protection. M.: Engineering, 2009. 507 p. (In Russ)]
2. Khorev A.A., Zashchita informatsii ot utechki po tekhnicheskim kanalim. Chast' 1. Tekhnicheskiye kanaly utechki informatsii. – M.: Gostekhkomiissiya RF, 1998. – 320 s. [Khorev AA, Protection of information from leakage through technical channels. Part 1. Technical channels of information leakage. - M.: State Technical Commission of the Russian Federation, 1998. -320 p. (In Russ)]
3. Kabanov A.S. Vremennaya model' otsenivaniya riska narusheniya informatsionnoy bezopasno-sti / A.S. Kabanov, A.B. Los', V.I. Truntsev // Doklady Tomskogo gosudarstvennogo univer-siteta sistem upravleniya i radioelektroniki. 2012. T. 1. № 25. S. 87-91. [Kabanov A.S. A temporary model for assessing the risk of information security breach / A.S. Kabanov, A.B. Moose, V.I. Truntsev // Reports of Tomsk State University of Control Systems and Radioelectronics. 2012.V. 1. No. 25. pp. 87-91. (In Russ)].
4. Khorev A.A., Sposoby i sredstva zashchity informatsii. Uchebnoye posobiye. – M.: MO RF, 2000. – 316 s. [Khorev AA, Methods and means of information protection. Tutorial. - M.: MO RF, 2000. 316 p. (In Russ)].
5. Torokin A.A.. Inzhenerno-tekhnicheskaya zashchita informatsii: Gelios ARV. – 2005, - 960s. [Torokin A.A. Engineering and technical information protection: Helios ARV. 2005, 960p. (In Russ)].
6. Buzov G.A. Zashchita ot utechki informatsii po tekhnicheskim kanalim : ucheb. posobiye / G.A. Bu-zov, S.V. Kalinin, A.V. Kondrat'yev. M.: Goryachaya liniya Telekom, 2014. 416 s. [Buzov G.A. Protection against information leakage through technical channels: textbook. allowance / G.A. Buzov, S.V. Kalinin, A.V. Kondratyev. M.: Hotline Telecom, 2014.416 p. (In Russ)]
7. Charaf H. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. pp. 277–282.
8. Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Sliwa // Entropy. 2014. Vol. 16. Issue 12. pp. 6602–6623.
9. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). 2016. pp. 133–187.
10. Pavlovskiy YU.N. Imitatsionnyye modeli i sistemy / YU.N. Pavlovskiy. — M.: Fazis: VTS RAN, 2000. — S. 134. [Pavlovsky Yu. N. Simulation models and systems / Yu. N. Pavlovsky. M.: Fazis: VC RAN, 2000. 134 p. (In Russ)].
11. Krasnoshchokov P.S. Optimizatsiya v avtomatizirovannom proyektirovanii / P.S. Krasnoshchokov, V.V. Morozov, N.M. Popov. M.: MAKSS Press, 2008. 323 s. [Krasnoshchekov P.S. Optimization in computer-aided design / P.S. Krasnoshchekov, V.V. Morozov, N.M. Popov. M.: MAKSS Press.] 2008. 323 p. (In Russ)]
12. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. pp. 1–5.
13. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114–118.
14. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. Vol. 94. pp. 1–24.

Сведения об авторах:

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; e-mail: aevgenirogozin@yandex.ru

Силка Дмитрий Григорьевич, инженер-электроник отдела информационно технического обеспечения учебного процесса; e-mail: sdg.silka@gmail.com

Гуляев Олег Анатольевич, генеральный директор, e-mail: aerovoskhod@sovintel.ru

Information about the authors:

Evgeny A. Rogozin, Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs; e-mail: aevgenirogozin@yandex.ru

Dmitry G. Silka, electronic engineer of the Department of Information and Technical Support of the Educational process; e-mail: sdg.silka@gmail.com

Oleg A.Gulyaev, General Director, e-mail: aerovoskhod@sovintel.ru

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию 15.10.2019.

Принята в печать 14.11.2019.

Conflict of interest.

The authors declare no conflict of interest.

Received 15.10.2019.

Accepted for publication 14.11.2019.