ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 2(28) / 2018

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

ISSN 2225-5435

UrFR Newslette

INFORMATION SECURITY

№ 2(28) / 2018

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

The journal « UrFR Newsletter. Information Security » is included in the List peer-reviewed scientific publications, in which should be published main scientific results of scientific dissertations degree of doctor and candidate of science

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

IN THIS ISSUE

УДК 621.396.6.019.3 + 004.056 Вестник УрФО № 2(28) / 2018, с. 5–10

Колкк А. А.

РАДИОЭЛЕКТРОННАЯ БОРЬБА В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ

В статье показана необходимость совершенствования средств радиоэлектронной борьбы в целях обеспечения выполнения задач информационного противоборства. Рассмотрены вопросы применения элементов искусственного интеллекта в системах распознавания типов радиоэлектронных средств (РЭС). Дано понятие «нечеткого» распознавания типа радиоэлектронных средств.

Ключевые слова: *информационная война, комплексы радиоэлектронного подавления, нечёткая логика, оптимальная фильтрация.*

Kolkk A. A.

ELECTRONIC WARFARE IN INFORMATION CONFRONTATION

Need of improvement of means of radio-electronic fight for ensuring performance of problems of information confrontation is shown in article. Questions of application of elements of artificial intelligence in the systems of recognition of types of radio-electronic means (RES) are considered. The concept of "fuzzy" recognition like radio-electronic means is given.

Keywords: *information war, complexes of radio-electronic suppression, fuzzy logic, optimum filtration.*

Информационное противоборство. Развитие мирового сообщества наглядно демонстрирует, что в последнее время критически важным государственным ресурсом, оказывающим все большее влияние на национальную безопасность, становится информация, циркулирующая в автоматизированных системах управления и связи. Данные системы являются неотъемлемым компонентом структуры управления государством, экономикой, финансами и обороной.

В сложившейся обстановке ряд развитых западных государств, и в первую очередь США, в начале 90-х годов вплотную приступили к изучению и проработке проблем, связанных с противоборством в информационной сфере, или так называемой «информационной войной» (ИВ) [1].

«Информационная война» – это комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных решений в интересах государства, а в ходе войны полностью парализовало структуру

управления противника. В ИВ кроме наступательной составляющей не менее важной является необходимость обеспечить надёжную защиту своей информационной структуры [2].

Победа в информационной войне иногда даже более значима, чем на поле боя. Множество вооружённых конфликтов начиналось с информационного противостояния. Первым этапом, которого являлась подготовка мировой общественности о необходимости решения «назревших проблем» в деятельности какого-либо государства, путём вброса дезинформации в мировые СМИ о нарушение данным государством существующих договоров, демократических основ, нарушение прав меньшинств и т.д. (Ирак, Ливия, и др.) Пропаганда со стороны США своей политики, насаждение своего понимания демократии, вмешательство во внутренние дела государств, применение вооружённых сил без санкции ООН – всё это требует ответных действий в информационной сфере со стороны России и других государств.

После окончания боевых действий информационная война продолжается и результат её иногда даже более важен, чем победа в вооружённом конфликте.

В наши дни мы являемся свидетелями того, что наряду с термином информационная война всё чаще применяется словосочетание «гибридная война» Это понятие отражает имеющиеся в наличии реалии применения инструментов борьбы и последних достижений в сфере соперничества стран.

«Гибридная война» – вид военного противоборства отдельных государств, которое вовлекает в вооруженный конфликт, кроме или вместо регулярной армии – спец миссии и спецслужбы, партизанские и наемные силы, террористические атаки, протестные массовые беспорядки [3]. При этом основной целью чаще всего является не оккупация и присвоение территории, а перемена политического режима или устоев государственной политики в стране, подвергаемой атаке. В качестве примера можно привести международные события последнего десятилетия (события вокруг Сирии, Украины).

Использование радиоэлектронных средств и ВТ может обеспечить военное превосходство на поле боя и нарушить все сферы жизни общества. Специалисты ставят средства информационной войны (ИВ) на второе место после оружия массового поражения (ОМП) по степени их разрушительного действия. Зарубежные эксперты считают, что в настоящее время нет готовых решений в организации надежной защиты от возможных средств радиоэлектронного воздействия.

Воздействие на радиоэлектронные объекты информационных систем противника осуществляется двумя путями – электромагнитным излучением и воздействием на информационные базы данных и специальное программное обеспечение ЭВМ в АСУ войсками и оружием. Обеспечивается традиционным оружием – средствами РЭБ.

Меры по обеспечению ИБ становятся все более необходимыми по мере расширения использования компьютеров и компьютерных сетей. Структура компьютерных сетей сейчас настолько сложна, что практически отсутствует возможность уверенно идентифицировать всех, имеющих к ним доступ.

Если противник выберет в качестве объекта атаки не военные, а незащищенные гражданские сети и банки данных, то последствия будут катастрофическими. Более 90% потоков передачи данных и телефонных разговоров Министерства обороны различных государств, в том числе США идет по гражданским системам телефонной связи. Весьма значительными могут быть также и экономические потери от информационной атаки на телефонные системы.

Роль и место радиоэлектронной борьбы в информационном противоборстве. Насыщенность радиоэлектронного оборудования (РЭО) в системах управления оружием, в том числе и высокоточного оружия (ВТО), повышает значимость РЭБ как вида боевого обеспечения. Спектр задач РЭБ расширяется и, сливаясь с другими боевыми задачами, ведет к перерастанию РЭБ в «информационную войну».

Анализ основных тенденций развития вооруженной борьбы позволил установить, что 30% рассматриваемых сегодня задач информационного противоборства мирного времени и не менее 60% задач военного времени взаимосвязаны с задачами, традиционно решаемыми радиоэлектронной борьбой. В большей степени, чем раньше, пересекаются объекты информационного воздействия и радиоэлектронной борьбы, так как первооснову перспективных информационных систем составляют радиоэлектронные средства – традиционные объекты РЭБ, следователь-

но, одно из доминирующих мест в информационном противоборстве принадлежит радиоэлектронной борьбе.

Целями радиоэлектронной борьбы в системе информационного противоборства являются:

– дезорганизация функционирования информационных систем противника, обеспечение устойчивой работы своих информационных систем;

– снижение возможностей противника по сбору информации о войсках, объектах базирования ВС, информационных системах с помощью технических средств.

В мирное время цели РЭБ это завоевание и удержание превосходства в информационной сфере, а в военное время – повышение эффективности боевых действий войск. Возникает необходимость совершенствования средств радиоэлектронного подавления (РЭП). Развитие средств РЭП идет в тесном взаимодействии с развитием радиоэлектронной техники и характеризуется постоянной технической и научной конфронтацией. Любое совершенствование радиоэлектронной техники, связанное с повышением ее эффективности, надежности и помехоустойчивости, вызывает ответную реакцию в области РЭП.

Перспективные радиоэлектронные системы снабжаются устройствами искусственного интеллекта, позволяющими в процессе работы анализировать электронную обстановку и вырабатывать наиболее оптимальные решения в отношении режимов работы.

Вместе с тем, используемая в современных системах (РЭП) логика управления обычно ограничивается заданными, (фиксированными) алгоритмами, которые при появлении новых, прогрессивных радиоэлектронных средств часто становятся бесполезными. Отсюда вытекает необходимость применения искусственного интеллекта в организации систем РЭП, в том числе бортовых, работающих в реальном режиме времени. Поэтому в перспективное оборудование РЭП желательно включать устройства, которые бы обладали способностью самообучения и подстройки алгоритмов в соответствии с изменяющейся обстановкой.

Одним из вариантов применения искусственного интеллекта в организации работы бортового комплекса РЭП является применение теоретических основ и прикладных методов современного научного направления – нечёткой логики.

Областью внедрения алгоритмов нечеткой логики являются всевозможные экспертные системы, в том числе: контроль над производственными процессами, самообучающиеся системы, исследование критических ситуаций; ***распознавание образов*** и др.

В отличие от традиционной математики, требующей на каждом шаге моделирования точных и однозначных формулировок закономерностей, нечеткая логика предлагает иной уровень, подход, при котором постулируется лишь минимальный набор закономерностей.

Нечеткие числа, получаемые в результате «не вполне точных измерений», во многом аналогичны распределениям теории вероятностей. В пределе, при возрастании точности, нечеткая логика приходит к стандартной, Булевой. По сравнению с вероятностным методом, нечеткий метод позволяет резко сократить объем производимых вычислений, что, в свою очередь, приводит к увеличению быстродействия нечетких систем.

Для комплексов РЭП одним из важных элементов является система радиотехнической разведки. Основной задачей данной системы является распознавание типа облучающей РЛС, т.е. идентификация объекта (РЛС). Решение данной задачи предполагается комплексированием методов фильтрации Калмана и нечёткой логики (НЛ).

На рис.1 представлена структурная схема станции радиотехнической разведки, использующей комплексирование методов ОФК и НЛ.

Пусть в некотором районе (информационном пространстве) обнаружена работа группы радиоэлектронных средств. Для каждого известного РЭС в соответствующей базе данных определены диапазоны возможной перестройки частоты и другие параметры. Для использования аппарата оптимальной фильтрации необходимо разработать динамико-стохастическую модель процесса эволюции параметров и модель процесса измерения [4].

Уравнения записываются для каждого типа РЭС из базы данных, и формируется так называемый банк фильтров Калмана. Обработка принятых сигналов происходит параллельно. Фильтр, параметры которого соответствуют принятому сигналу, даёт сходящуюся оценку при минимуме ковариационной матрицы и невязки (обновляющего процесса).

Для разрешения ситуации неопределенности, когда координаты вектора измерения

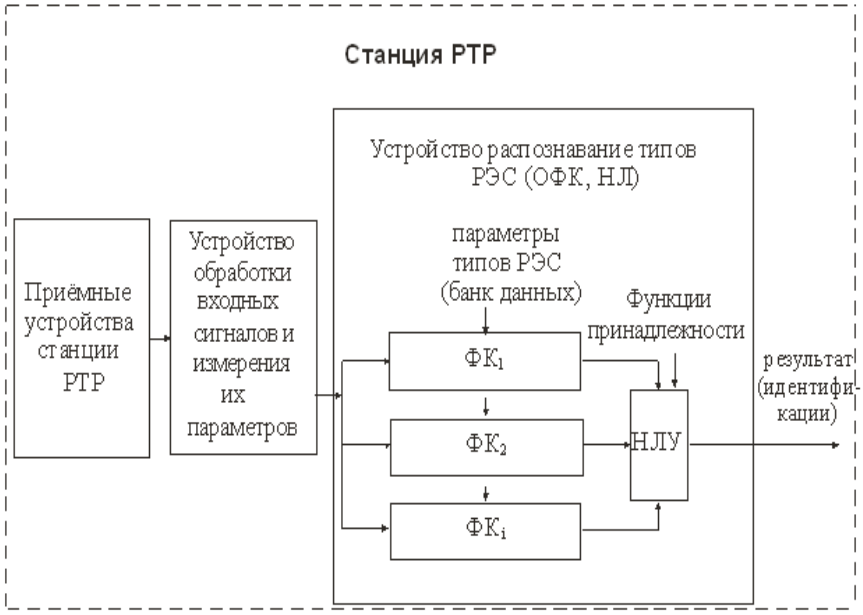

Рис. 1. Структурная схема станции радиотехнической разведки с устройством распознавания типов, использующего комплексирование методов ОФК и НЛ

попадают одновременно в несколько областей предполагаемых РЭС предлагается использовать методы нечёткой логики.

Рассмотрим понятие «нечеткой» идентификации объекта, как следствие, «нечеткого» распознавания типа РЭС, которое понимается как попадание вектора состояния в пространство принадлежности РЭС, относящееся к 2 типам РЭС одновременно. Понятие нечеткой идентификации объекта достаточно хорошо отражает сложившийся на практике экспертный подход [4]. Действительно, эксперт, руководствуясь значением вектора состояния, который определяет принадлежность к тому или иному типу, может считать, что объект принадлежит к типу А или принадлежит к «другому» типу, если значение вектора состояния находится вне пространства принадлежности данному РЭС. Причем в зависимости от конкретного значения разности между измеренными параметрами вектора состояния и параметрами, заложенными в банке экспертов для данного типа, можно считать, что объект принадлежит к типу А или не принадлежит данному типу соответственно в разной степени [5].

Определим нечеткую идентификацию объекта по вектору состояния как лингвистическую переменную, характеризующуюся, например, двумя термами (нечеткими множествами) – тип А или «другой» тип, которые описываются соответствующими функциями принадлежности $\mu^0_{v_i}$ и $\mu^1_{v_i}$.

На рис.2 приведена иллюстрация понятий «четкой» (а) и «нечеткой» (б) идентификации объекта. В первом случае области значений вектора состояния *xi*, соответствующие типу А и не соответствующие типу А (на рисунке они обозначены прямоугольниками разной окраски), разделены четкой границей. Во втором случае эти области пересекаются (область пересечения отмечена штриховкой) и описываются соответствующими функциями принадлежности с параметрами «a» и «b». В результате при любом значении вектора $x = xi$ состояние процесса (распознавания) может быть соотнесено как с нечетким множеством типа А ($\mu^0_{v_i} = 0{,}8$) , так и с нечетким множеством, не принадлежащим типу А ($\mu^1_{v_i} = 0{,}3$).

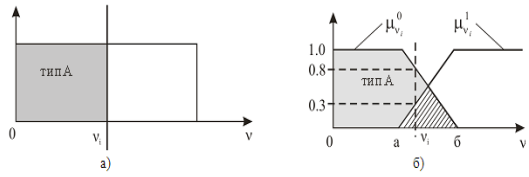

Рис.2. Иллюстрация понятий а) «чёткой» и б) «нечёткой» идентификации объекта

Заметим, что в настоящей работе рассмотрение ограничено использованием кусочно-линейных функций принадлежности, таких как трапецеидальная, треугольная и в данном случае Z- образная

Предполагается, что невязка *vi, i=0,N*, формируемая на выходе *i*-го фильтра Калма-

$$\mu_{v_i}^0 = \begin{cases} 1. & 0 \le f \le a. \\ \dfrac{b-f}{b-a}. & a \le f \le b. \\ 0. & \text{äðóãîå} \end{cases} \quad \mu_{v_i}^1 = \begin{cases} 0. & 0 \le f \le a. \\ \dfrac{f-a}{b-a}. & a \le f \le b. \\ 1. & \text{äðóãîå} \end{cases}$$

на (ФК), может быть представлена лингвистической переменной, например, с двумя термами – «малая» и «большая», для которых заданы функции принадлежности $\mu_{v_i}^0$ и $\mu_{v_i}^1$ *i= 0, N* [6].

Терм «малая» соответствует ситуации, когда на выходе фильтра невязка мала, т.е. измеренный вектор состояния близок вектору состояния предполагаемого типа РЭС. Появление хотя и малого, но не нулевого значения этой невязки объясняется переходными процессами, сопровождающими оценивание, отсутствием на практике полной адекватности используемой при синтезе наблюдателя модели системы распознавания, неучтенными возмущениями ее динамики или выхода. Терм «большая» соответствует ситуации, когда измеренный вектор состояния, существенно отличается от вектора состояния ФК i-го наблюдателя. Так бывает, если, например, на вход ФК i-го наблюдателя поступает сигнал с параметрами присущими j–му наблюдателю. При этом параметры *{ai,bi | i = 0,N}* функций принадлежности определяются равенствами:

$$a_i = \min_i \left\{ v_i \middle| S_j, j \ne i \right\},$$

$$b_i = \max_i \left\{ v_i \middle| S_j, j = i \right\}$$

С помощью элементов нечёткой логики в программных средах MatLab (расширение Fuzzy Logic Toolbox) и FuzzyTECH создана нечёткая модель «Распознавание типов РЭС», основанная на базе знаний экспертов, учитывающая изменения оперативной обстановки и появление новых РЭС, а также позволяющая принимать решение по каждому полученному сигналу (измеренным его параметрам).

Совершенствование комплексов РЭП, в том числе методами нечёткой логики, необходимо для поддержания паритета в области ИВ (гибридных) и, далее обеспечить преимущество в ведении информационного противоборства, в решении его задач по дезорганизации функционирования систем управления и защите своих аналогичных систем.

Литература

1. Гриняев С. Н. Взгляды военных экспертов США на ведение информационного противоборства/ С. Н. Гриняев //Зарубежное военное обозрение, 2001. – № 8. – С. 10–12.

2. Жуков В. Взгляды военного руководства США на ведение информационной войны. / В. Жуков. //Зарубежное военное обозрение, 2001. – № 1. – С. 2–9.

3. Позубенков П. С., Позубенков С. П. Гибридные войны в современном информационном пространстве /П. С. Позубенков // Научно-методический электронный журнал «Концепт», 2016. – Т. 11. – С. 1121–1125.О.

4. Горнов А.Ю., Даровских С.Н., Жолудев А.И., Тятюшкин А.И., Хаютин М.И., Ширяев В.И. Опыт применения пакета прикладных программ к задаче оптимального управления маневрирующим летательным аппаратом. //Интеллектуализация программных средств. – Новосибирск: Наука. Сиб. Отд-ние, 1990. – С. 152-160.

5. Безмен Г.В., Колесов Н.В. Функциональное диагностирование динамических систем с использованием нечетких правил анализа и принятия решений об отказе / Г.В. Безмен // Известия РАН. Теория и системы управления, 2011. – № 3. – С. 3–12.

6. Колкк А.А., и др. Об алгоритмах распознавания типов радиоэлектронных средств в бортовых комплексах разведки: сб. науч. ст. по материалам II Всероссийской НПК «АВИАТОР» (11-13 февраля 2015г.) Актуальные вопросы исследований в Авионике: теория, обслуживание, разработки: В 2-ух т. Т.2. Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 86-92.

References

1. Grinyaev S. N. Vzglyady voennyh ehkspertov SSHA na vedenie informacionnogo protivoborstva/ S. N. Grinyaev //Zarubezhnoe voennoe obozrenie, 2001 – no 8. – pp. 10–12.

2. Zhukov V. Vzglyady voennogo rukovodstva SSHA na vedenie informacionnoj vojny. / V. Zhukov. // Zarubezhnoe voennoe obozrenie, 2001. – no 1. – pp. 2–9.

3. Pozubenkov P. S., Pozubenkov S. P. Gibridnye vojny v sovremennom informacionnom prostranstve /P. S. Pozubenkov // Nauchno-metodicheskij ehlektronnyj zhurnal «Koncept», 2016. – vol. 11. – pp. 1121–1125.

4. Gornov A.YU., Darovskih S.N., Zholudev A.I., Tyatyushkin A.I., Hayutin M.I., Shiryaev V.I. Opyt primeneniya paketa prikladnyh programm k zadache optimal'nogo upravleniya manevriruyushchim letatel'nym apparatom. //Intellektualizaciya programmnyh sredstv. – Novosibirsk: Nauka. Sib. Otd-nie, 1990. – pp. 152-160.

5. Bezmen G.V., Kolesov N.V. Functional Diagnosis of Dynamic Systems Using Fuzzy Rules Analysis and Decision Making on Refusal/ G.V Bezmen //Izvestiya RAN. Theory and Control Systems, 2011. – no. 3. – pp. 3–12.

6. Kolkk A.A., i dr. Ob algoritmah raspoznavaniya tipov radioehlektronnyh sredstv v bortovyh kompleksah razvedki: sb. nauch. st. po materialam II Vserossijskoj NPK «AVIATOR» (11-13 fevralya 2015g.) Aktual'nye voprosy issledovanij v avionike: teoriya, obsluzhivanie, razrabotki: v 2-uh t. vol.2. Voronezh: VUNC VVS «VVA», 2015. – pp. 86-92.

КОЛКК Андрей Александрович, преподаватель 13 кафедры авиационных комплексов и конструкции летательных аппаратов филиала ВУНЦ ВВС ВВА в 454015 г. Челябинск, E-mail: kandidatyra@mail.ru

KOLKK Andrey, lecturer of the Department of 13 aircraft systems and aircraft design branch VUNTS VVS VVA 454015 in Chelyabinsk. E-mail: kandidatyra@mail.ru

УДК 621.396.621/.65 Вестник УрФО № 2(28) / 2018, с. 11–15

Савашинский И. И., Астрецов Д. В.

СКРЫТНОЕ УСТРОЙСТВО РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ ИЗМЕРИТЕЛЕЙ СКОРОСТИ ДВИЖЕНИЯ ТРАНСПОРТНЫХ СРЕДСТВ И МЕТОДЫ РАДИОЭЛЕКТРОННОЙ ЗАЩИТЫ

Объектами исследования данной работы являются измеритель скорости движения транспортных средств «Искра-1», радар-детектор Escort Passport 9500ix, скрытное устройство для радиоэлектронного подавления измерителей скорости движения транспортных средств. Цель работы состоит в формировании принципов работы скрытного устройства для радиоэлектронного подавления измерителей скорости движения транспортных средств и описании методов радиоэлектронной защиты. В данной работе учитывались ранее опубликованные работы [1,2,3], связанные с измерителем скорости движения транспортных средств «Искрой-1» – его технические характеристики, принцип действия и конструкция, а также с радар-детектором Escort Passport 9500ix – его возможности и режимы работы. Данная работа является уникальной в своем роде, т.к. скрытное устройство для радиоэлектронного подавления измерителей скорости движения транспортных средств в других работах автором не встречалось. В результате работы сформированы принципы работы скрытного устройства для радиоэлектронного подавления измерителей скорости движения транспортных средств и описаны методы радиоэлектронной защиты.

Ключевые слова: *Скрытное устройство, радиоэлектронное подавление (РЭП), измеритель скорости движения транспортного средства (ТС), радиоэлектронная защита (РЭЗ), радар-детектор.*

Savashinskiy I. I., Astrecov D. V.

VEHICLES SPEED MEASUREMENT SYSTEMS RADIO-ELECTRONIC REPRESSION SECRETIVE DEVICE AND RADIO-ELECTRONIC PROTECTION METHODS

This work research objects are the following: vehicles speed measurement system «Iskra-1», radar-detector Escort Passport 9500ix, vehicles speed measurement systems radio-electronic repression secretive device. This work purpose is the following: vehicles speed measurement systems radio-electronic repression secretive device working principals formation and radio-electronic protection methods description. In this work previously published works [1,2,3] connected with vehicles speed measurement system «Iskra-1» – its technical characteristics, working principal and construction – and radar-detector Escort Passport 9500ix – its possibilities and working modes – are taken into consideration. This work comes as unique one of its kind because of vehicles speed measurement systems radio-electronic repression secretive device doesn't review in other works previously. As a result of this work vehicles speed measurement systems radio-electronic repression secretive device working principals are formed and radio-electronic protection methods are described.

Keywords: *secretive device, radio-electronic repression (RER), vehicles speed measurement system, radio-electronic protection (REP), radar-detector.*

Обзор литературы на тему «Радиоэлектронное подавление» позволяет убедиться в значительном количестве теоретических источников и практических работ, связанных с радиоэлектронным подавлением – его основными особенностями и недостатками, методами формирования и обнаружения, а также со временем и местом применения конкретных его видов. Но все это многообразие собрано в одной единственной предметной области и развивается в одном единственном направлении – вооруженные силы – по крайней мере, так можно судить исходя из информации в свободном доступе.

Вышесказанное показывает актуальность формирования методов радиоэлектронной защиты измерителя скорости движения транспортных средств «Искра-1» при радиоэлектронном подавлении скрытным устройством. Что касается оригинальности данной работы, то при радиоэлектронном подавлении скрытным устройством известное решение по устранению сигнала по одной из координат применяется в предметной области, не связанной с вооруженными силами – радиоэлектронном подавлении измерителей скорости движения транспортных средств.

Во-первых, обозначим основные этапы расчета параметров помехи, используемой подавителем [1]:

1. Определение рабочего отношения мощности сигнала к мощности шума на входе приемника измерителя $q_{раб}^2$ при отсутствии на входе помехи подавителя ($P_{прав}$=0.95);

2. Определение мощности собственных шумов приемника измерителя $P_ш$ с использованием зависимости шумов приемных устройств от несущей частоты. См. рис. 1;

3. Определение рабочего отношения мощности сигнала к мощности шума на входе приемника измерителя $q_{раб'}^2$ при присутствии на входе помехи подавителя ($P_{прав'}$=0.05);

4. Определение мощности ответной имитационной уводящей помехи $P_{ш'}$ приведенной ко входу приемника измерителя.

Во-вторых, обозначим основные этапы

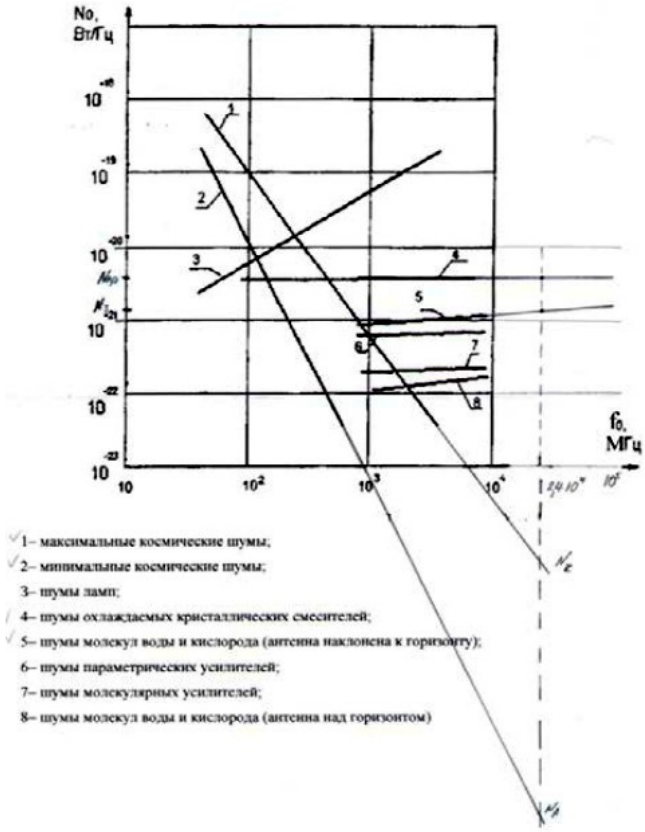

Рис. 1. Зависимости шумов приемных устройств от несущей частоты

проектирования рупорно-линзовой антенны измерителя [2]:

1. Определение коэффициента затухания α' волны E_{01} в круглом стандартном волноводе с учетом его длины;

2. Определение коэффициентов усиления рупорно-линзовой антенны измерителя при использовании ее как передающей $(\eta_{пер}=0.95)\ D_{пер}$ и как приемной $(\eta_{пр}=0.45)\ D_{пр}$.

В-третьих, обозначим основные этапы проектирования резонансной многощелевой антенны подавителя:

1. Определение ширины всех щелей $d_щ$;

2. Определение продольной и наклонной длины всех щелей $l_щ$;

3. Определение числа щелей N;

4. Определение габаритных размеров а (узкая стенка), b (широкая стенка) и L (итоговая длина) прямоугольного волновода многощелевой антенны с использованием номограммы для расчета многощелевых антенн при π способе возбуждения. См. рис. 2;

5. Определение коэффициента усиления $D_щ$.

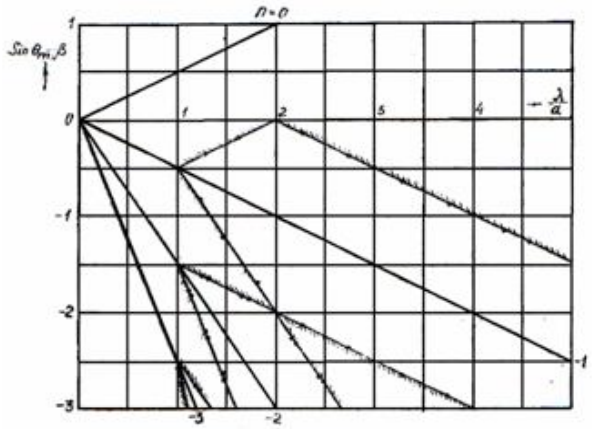

Рис. 2. Номограмма для расчета многощелевых антенн при π способе возбуждения

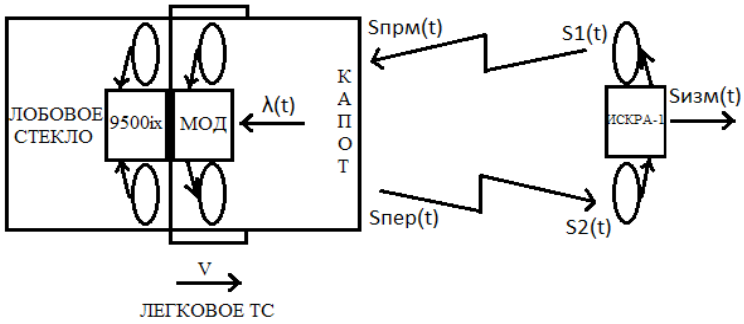

Рис. 3. Ситуационная схема

В-четвертых, приведем ситуационную схему, поясняющую принципы работы скрытного устройства для РЭП измерителей скорости движения ТС:

Здесь же приведем все соотношения имеющие место на указанной выше ситуационной схеме:

$$S_1(t) = U_0\cos(\omega_0 t + \varphi_0),$$

$$S_{ПРМ}(t) = U_1\cos(\omega_0 t + \Omega_Д t + \varphi_1),$$

$$S_{ПЕР}(t) = U_2\cos(\omega_0 t + \Omega_Д t + \lambda(t) + \varphi_2),$$

$$S_2(t) = U_3\cos(\omega_0 t + 2\Omega_Д t + \lambda(t) + \varphi_3),$$

$$S_{ИЗМ}(t) = U_4\cos(2\Omega_Д t + \lambda(t) + \varphi_4),$$

где S_i – соответствующий сигнал,

U_i – амплитуда соответствующего сигнала,

ω_0 – частота излучаемого «Искрой-1» сигнала $S_1(t)$,

φ_i – фаза соответствующего сигнала,

$\Omega_Д$ – частота Доплера,

$\lambda_{(t)}$ – ФМ сигнал, возбуждающий капот.

А также сформируем принципы работы скрытного устройства для РЭП измерителей скорости движения ТС:

1. Легковое ТС преодолевает «Искру-1» с превышением установленного скоростного режима вплоть до 180км/ч: для заблаговременного обнаружения сигнала «Искры-1» используем Escort Passport 9500ix – «Искра-1» измеряет скорость на расстоянии 800м, Escort Passport 9500ix обнаруживает «Искру-1» на расстоянии 1800м [3];

2. С момента обнаружения «Искры-1» автоматически активируется скрытное устройства для РЭП, возбуждая капот легкового ТС, используемый в роли приемной и передающей (переизлучающей) антенны в силу наличия под ним многощелевой антенны, ФМ сигналом λ(t) с частотой, достаточной для увеличения составляющей $\Omega_Д t$ до значения вне пределов измеряемого «Искрой-1» частотного диапазона;

3. При достижении легковым ТС расстояния в 800м до «Искры-1», последняя излучает сигнал $S_1(t)$, который принимается капотом легкового ТС как $S_{ПРМ}(t)$, после чего сигнал отражается (переизлучается) капотом легкового ТС как SПЕР(t) с необходимой добавкой λ(t) и принимается «Искрой-1» как сигнал $S_2(t)$, которая в итоге по сигналу $S_{ИЗМ}(t)$ и определяет превышение установленного скоростного режима. См. рис. 3.

В заключение, опишем методы РЭЗ:

Одним из важных факторов РЭЗ является то, что значения средней частоты помехи и сигнала всегда различны. При создании активных помех минимальная ошибка настройки передатчика помех сопоставима с полосой пропускания приемника подавляемой радиолокационной системы. Если в приемнике применяется, например, когерентная обработка сигналов, то различие частот сигнала и помехи может способствовать существенному снижению эффективности помех.

Большое значение для РЭЗ может иметь также случайность положения помеховых импульсов на временной оси: применение, например, схем чересперидного суммирования может существенно улучшить отношение сигнал/помеха.

Существенным обстоятельством при РЭЗ является синхронность огибающих помеховых импульсов относительно начала отсчета времени в радиолокационной системе. В то же время помеха имеет ряд отличий от полезных сигналов. Как правило, имеет место существенное превышение помехи над сигналом по амплитуде (мощности). Следовательно, большое значение для защиты от помех приобретает амплитудная селекция.

Литература

1. И.И. Савашинский. Active masking noise energy parameters finding used for vehicles speed measurement system "Iskra-1" radio-electronic repression. Инновационный центр развития образования и науки. Международная научно-практическая конференция «Технические науки в мире: от теории к практике». Ростов-на-Дону, 2016, в. 3, стр. 76-81.

2. И.И. Савашинский. Active masking noise no energy parameters finding used for vehicles speed measurement system "Iskra-1" radio-electronic repression. Научно-издательский центр «Академический». IX Международная научно-практическая конференция «Наука в современном информационном обществе». North Charleston (USA), 2016, стр. 113-115.

3. И.И. Савашинский. Effective vehicles speed measurement system "Iskra-1" radio-electronic repression. Федеральный центр науки и образования «Эвенсис». Международная научно-практическая конференция «Современные достижения и разработки в области технических наук». Хабаровск, 2016, в. 1, стр.51-55.

References

1. I.I. Savashinskiy. Active masking noise energy parameters finding used for vehicles speed measurement system "Iskra-1" radio-electronic repression. Innovatsionnyy tsentr razvitiya obrazovaniya i nauki. Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Tekhnicheskiye nauki v mire: ot teorii k praktike». Rostov-na-Donu, 2016, v. 3, str. 76-81.

2. I.I. Savashinskiy. Active masking noise no energy parameters finding used for vehicles speed measurement system "Iskra-1" radio-electronic repression. Nauchno-izdatel'skiy tsentr «Akademicheskiy». IX Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Nauka v sovremennom informatsionnom obshchestve». North Charleston (USA), 2016, str. 113-115.

3. I.I. Savashinskiy. Effective vehicles speed measurement system "Iskra-1" radio-electronic repression. Federal'nyy tsentr nauki i obrazovaniya «Evensis». Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Sovremennyye dostizheniya i razrabotki v oblasti tekhnicheskikh nauk». Khabarovsk, 2016, v. 1, str.51-55.

САВАШИНСКИЙ Илья Игоревич, бакалавр с отличием ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина» департамента «Радиоэлектроника и связь» ИРИТ-РтФ. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: egor37-ilya14@yandex.ru

АСТРЕЦОВ Дмитрий Вячеславович, кандидат технических наук, профессор, профессор ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина» департамента «Радиоэлектроника и связь» ИРИТ-РтФ. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: egor37-ilya14@yandex.ru

SAVASHINSKIY Ilya, golden bachelor of The UrFU named after the first President of Russia B.N. Yeltsin of The Radio-electronics and communication Department IRIT-RTF. 620002, Yekaterinburg, Mira, 19. E-mail: egor37-ilya14@yandex.ru

ASTRECOV Dmitriy, candidate of technical sciences, professor, professor of The UrFU named after the first President of Russia B.N. Yeltsin of The Radio-electronics and communication Department IRIT-RTF. 620002, Yekaterinburg, Mira, 19. E-mail: egor37-ilya14@yandex.ru

УДК 004.048 + 621.396.6.049.77 Вестник УрФО № 2(28) / 2018, с. 16–18

Швырев Б. А., Бердник М. В.

ХАРАКТЕРИСТИКА ПРИЁМНИКА СИГНАЛА, ПЕРЕИЗЛУЧЕННОГО ПАССИВНОЙ РАДИОЗАКЛАДКОЙ

Используя метод возмущенного поля рассматривается работа пассивной радиозакладки, образующей акустический канал утечки информации. Выполняется синтез приемника переизлученного радиозакладкой сигнала и определения его характеристики. Анализируются рабочие характеристики приёмника.

Ключевые слова: *акустический канал утечки, пассивная радиозакладки, синтез приёмника, рабочие характеристики приемника.*

Shvyrev B. A., Berdnik M. V.

CHARACTERISTICS OF THE SIGNAL RECEIVER RE-EMITTED BY A PASSIVE RADIO PAD

Using the perturbed field method, the operation of a passive radio pad, which forms an acoustic channel for information leakage, is considered. The receiver is synthesized by a signal re-radiated by the radio-pad signal and its characteristic is determined. The performance characteristics of the receiver are analyzed.

Keywords: *acoustic leak channel, passive radio locks, receiver synthesis, receiver performance.*

В методе возмущенного поля используются радиомаяки, которые осуществляют модуляцию переотражённого сигнала, падающего на их поверхность[1]. Благодаря наличию параметрической модуляции с помощью управляемого пассивного маяка можно определить характеристики электромагнитного поля в месте его расположения. Управляемый пассивный маяк может быть использован не только для измерения характеристик поля, но и для определения координат объекта носителя пассивного радиомаяка. Управляя маяком низкочастотным информационным сигналом с микрофона позволит организовать акустический канал утечки информации. Управляемый информационным акустическим сигналом пассивный радиомаяк не имеет самостоятельного излучения, а поэтому не расходует энергии на её формирование. Энергия маяка используется лишь на изменение его электродинамических параметров, что позволяет рассматривать его как экономичное или даже энергонезависимое устройство – пассивную радиозакладку. Отсутствие сосредоточенной энергии делает радиозакладку незаметной при анализе радиоэфира.

Ещё одна важная характеристика радиозакладки это дальность его размещения от приемного устройства или дальность его обнаружения или передачи сообщения. Дальность обнаружения зависит от модуляции передающего устройства, модуляционных свойств управляемой пассивной радиоза-

кладки и от чувствительности приёмного устройства. С увеличением чувствительности приёмного устройства растёт и дальность, на которой он может передавать информацию.

Для оценки этой характеристики управляемой пассивной радиозакладки используемой в методе возмущенного поля выберем тип переизлучающей пассивной радиозакладке в виде диода-диполя [2]. Будем считать, что на эту пассивную радиозакладку падает совершенный гармонический сигнал. От управляющего источника информационного сигнала на диод, выводы которого играют роль полуволнового вибратора, подается напряжение, осуществляющее изменение параметров отражающего вибратора. При замыкании диода положительным напряжением получаем отражение от полуволнового вибратора, при размыкании отрицательным напряжением получаем отражение от двух четвертьволновых вибраторов. Различие эффективных поверхностей рассеивания полуволнового и четвертьволновых вибраторов вызывает модуляцию переизлученного управляемым пассивной радиозакладкой сигнала, что и позволяет выделить сигнал именно от него на фоне переотражений от других объектов не обладающих модуляционными возможностями.

Кроме информационного сигнала в приёмном устройстве присутствуют шумы имеющие тепловую и дробовую природу, которые будем считать белым гауссовским шумомn(t) с одностороннеё спектральной плотностью N0.

Для построения оптимального приёмника, обрабатывающего реализацию случайного сигнала ξ(t)сформулируем две гипотезы:

H_0 - $\xi(t)=A_1\cos(\omega_0 t+\varphi_1)+n(t)$, в принимаемой реализации ξ(t)содержится фоновое излучение отраженное от сторонних предметов и белый шум, где A_1,φ_1- неизвестные амплитуда и фаза фонового сигнала, а ω_0 - известная центральная частота сигнала;

H_1 - $\xi(t) = A_1\cos(\omega_0 t+\varphi_1) + A_2 (1+M\cos\Omega t) \cos(\omega_0 t+\varphi_2) + n(t)$, в принимаемой реализации помимо двух вышеупомянутых сигналов присутствует и сигнал от управляемой пассивной радиозакладки, с неизвестными параметрамиA_2, φ_2, с амплитудной модуляцией, имеющей глубину модуляции M и частоту Ω.

Синтез оптимального приёмного устройства в такой постановке задачи выполнен в работе [3] и алгоритм обработки реализации имеет вид

$$\frac{2N_0}{M^2T}[(X_2-X_1)^2+(Y_2-Y_1)^2] \lessgtr h \ , \quad (1)$$

где T– время наблюдения сигнала,

$$X_1 = \frac{2}{N_0}\int_0^T \xi(t)\cos\omega_0 t dt \ ;$$

$$X_2 = \frac{2}{N_0}\int_0^T \xi(t)(1+\mathrm{M}\cos\Omega t)\cos\omega_0 t dt \ ;$$

$$Y_1 = \frac{2}{N_0}\int_0^T \xi(t)\sin\omega_0 t dt \ ;$$

$$Y_2 = \frac{2}{N_0}\int_0^T \xi(t)(1+\mathrm{M}\cos\Omega t)\sin\omega_0 t dt \ ;$$

h – порог для сравнения. При превышении порога hвыходным сигналом приёмника принимается решение, что в реализацииξ(t) присутствует сигнал управляемой пассивной радиозакладки, при не превышении порога принимается решение, что в реализации ξ(t) сигнал пассивной радиозакладки отсутствует.

Найдем рабочие характеристики приёмника построенного в соотвествии с алгоритмом (1). Для удобства вычислений характеристик приведем (1) к виду

$$\eta = \sqrt{(\xi_1^2+\xi_2^2)} \lessgtr h_0, \ (2)$$

где

$$\xi_1 = \frac{2\sqrt{2}}{\sqrt{N_0 T}}\int_0^T \xi(t)\cos\Omega t\cos\omega_0 t dt \ ;$$

$$\xi_2 = \frac{2\sqrt{2}}{\sqrt{N_0 T}}\int_0^T \xi(t)\cos\Omega t \sin\omega_0 t dt \cdot$$

Найдем статистику η если ξ_1 и ξ_2 гауссовские случайные величины. Для этого найдем средние значения и дисперсии ξ_1 и ξ_2 при выполнении гипотезы H_0 .

$$<\xi_1>=<\xi_2>=0$$

Дисперсии при гипотезе H0равны

$$\sigma_1^2 = \sigma_2^2 =<\xi_1^2>=<\xi_2^2>=1$$

Известно[4], что при таких значениях параметров ξ_1 и ξ_2 величина η описывается релеевским распределением

$$W_0(x) = x exp(-x^2/2)$$

Вероятность ложной тревоги α, определяющая пороговый уровень h_0 равна

$$\alpha = \int_{h_0}^{\infty} x exp(-x^2/2)dx = \exp(-h_0^2/2), \quad h_0 = \sqrt{-2ln\alpha} \ .$$

При гипотезе H1 среднее значение ξ_1 и ξ_2 равны

$$<\xi_1>= MA_{02}\cos\varphi_{02}\sqrt{T/2N_0};$$

$$< \xi_2 >= MA_{02} \sin\varphi_{02}\sqrt{T/2N_0},$$

где A_{02}, φ_{02} – истинные значения фазы и амплитуды информационного сигнала управляемой пассивной радиозакладки.

Дисперсии при гипотезе H_1 имеют значения

$$\sigma_1^2 = \sigma_2^2 = 1$$

Известно [4], что в этом случае величина η имеет обобщенное релеевское распределение

$$W_1(x) = x exp(-(x^2 + z^2)/2)\, I_0(zx),$$

где $z^2 = M^2 A_{02}^2 T/2N_0$ – отношение сигнал-шум для сигнала управляемой пассивной радиозакладки, $I_0(zx)$ – модифицированная функция Бесселя нулевого порядка. Тогда рабочая характеристика приёмника – вероятность правильного обнаружения равна

$$P_D = \int_{h_0}^{\infty} x exp(-(x^2 + z^2)/2)\, I_0(zx) - x$$

Значения функции P_D рассчитаны в [5]. Выражение для PDпоказывает, что рабочие характеристики приёмника зависят только от отношения сигнал-шум сигнала управляемой пассивной радиозакладки. Для обеспечения роста отношения сигнал сигнал-шум необходимо увеличивать глубину модуляции сигнала M осуществляемую диодом радиозакладки и амплитуду облучающего высокочастотного радиосигнала.

Литература

1. Голография. Методы и аппаратура./ Под ред. В.М. Гинзбург, Б.М. Степанова. - М.: Сов. радио, 1974

2. А.Н. Лукин, Ю.И. Гридин, И.Ф. Струков. Устройство регистрации радиоголограмм и радиоизображений в реальном масштабе времени. Приборы и техника эксперимента, 1986. №4

3. А.В.Мальцев, Г.В.Степанов Синтез приёмника для обнаружения сигнала управляемого диода-диполя. Материалы открытой конференции "Актуальные проблемы деятельности подразделений УИС".- Воронеж, 2008.

4. В.И.Тихонов Оптимальный прём сигналов.- М.: Радио и связь,1983.

5. Таблицы распределения Релея –Райса / Л.С.Барк, Л.Н.Большев, П.И.Кузнецов, А.П.Черенков.- М.: ВЦ АН СССР,1964.

Reference

1.Golography. Methods and equipment. Ed. V.M. Ginzburg, B.M. Stepanova. - Moscow: Sov. radio, 1974

2. A.N. Lukin, Yu.I. Gridin, I.F. Strukov. A device for recording radio holograms and radio images in real time. Devices and experimental technique, 1986. №4

3. AVMaltsev, GV Stepanov Synthesis of a receiver for detecting a signal of a controlled diode-dipole. Materials of the open conference "Actual problems of the activities of the MIS units." - Voronezh, 2008.

4. V.I. Tikhonov Optimal signaling of signals. - Moscow: Radio and Communication, 1983.

5. Tables of the Rayleigh-Rice distribution / LSBark, LNBolshev, PI Kuznetsov, APChechenkov .-Moscow: VTS AN SSSR, 1964.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская,2. E-mail: bor2275@yandex.ru

БЕРДНИК Мария Викторовна, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская,2. E-mail: marviktr@mail.ru

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2 Moskovskaya street. E-mail: bor2275@yandex.ru

BERDNIK Maria, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2 Moskovskaya street. E-mail: marviktr@mail.ru

УДК 534.6 Вестник УрФО № 2(28) / 2018, с. 19–24

Асяев Г. Д., Антясов И. С.

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ШУМОВЫХ "РЕЧЕПОДОБНЫХ" ПОМЕХ ДЛЯ ЗАЩИТЫ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

В статье рассмотрены основные виды генераторов шума, проведено исследование применимости использования средства акустического зашумления, основанного на использовании в качестве шума "речеподобной" помехи. Произведён формантный метод расчёта разборчивости речи при использовании средств акустического зашумления. Проведено сравнение шумовых помех, выявлена наиболее эффективная разновидность шумовой "речеподобной" помехи. Определен минимальный уровень шума для достижения заданного уровня словесной разборчивости.

Ключевые слова: *защита информации, генератор шума, "речеподобная" помеха, разборчивость речи.*

Asyaev G. D., Antyasov I. S.

ESTIMATION OF THE EFFECTIVENESS OF THE USE OF "SPEECH-LIKE" NOISE FOR THE PROTECTION OF ACOUSTIC INFORMATION

The main types of noise generators are considered in the article, the applicability of the use of a noise generator based on the use of "speech-like" noise as noise is investigated. A formant method is used to calculate the intelligibility of speech when using acoustic noise. Comparison of noise interference, the most effective type of noise "speech-like" noise is revealed. A minimum noise level is determined to achieve a given level of verbal intelligibility.

Keywords: *information protection, noise generator, "speech-like" noise, intelligibility of speech.*

Из всего множества технических каналов утечки информации (ТКУИ) акустические каналы утечки речевой информации занимают особое место и остаются актуальным в настоящее время1. Они могут возникать при обсуждении информации ограниченного распространения в защищаемых помещениях при наличии трех составляющих:

– источник информации (люди, технические средства);

– среда распространения (воздушная, ограждающие конструкции);

– технические средства акустической разведки (ТСАР).

Акустическая (речевая) информация может быть перехвачена с помощью портативных устройств звукозаписи, электронных устройств негласного получения информации, направленных микрофонов и непреднамеренного прослушивания. Основной задачей пассивных средств защиты речевой информации является уменьшение соотношения сигнал/шум в возможных точках перехвата информации за счёт ослабления информативного сигнала. Средствами пассивной защиты являются: использование акустически неоднородных конструкций, установка фальшь-потолка, двойного тамбура и т.д. Если реализация пассивных архитектурно-строительных методов защиты является недостаточной, применяют активные технические средства защиты акустической информации, основной задачей которых является создание маскирующих помех с использованием генераторов шума. Основными целями защиты акустической информации является маскировка смыслового содержания и тематики разговора в защищаемом помещении.

В настоящее время для защиты помещений применяют генераторы белого и розового шума, основной задачей которых является превышение уровня шума над информативным сигналом. Проанализировав рынок защиты акустической информации, было замечено, что белый шум является самым распространённым видом помехи генерируемым средством активного зашумления. Его линейная характеристика располагается горизонтально во всем частотном диапазоне и обладает равномерной спектральной плотностью мощности. Розовый шум характеризуется уменьшением спектральной плотности мощности на 3 дБ к области высоких частот (рис. 1). Равномерномаскирующий шум сочетает в себе белый (0-500 Гц) и розовый шум (более 500 Гц)[2].

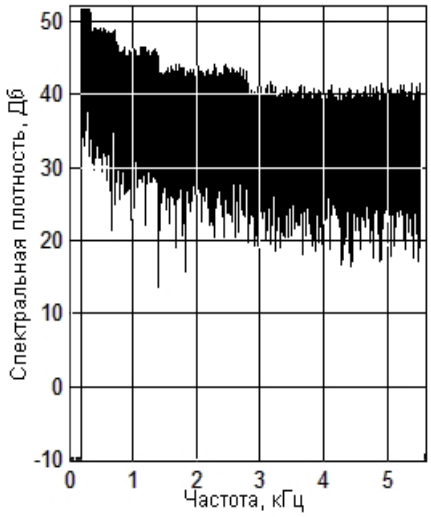

Рис. 1. Спектр розового шума

В отличие от белого шума, применение шумовых “речеподобных” помех позволяет замаскировать только определённый диапазон частот для защиты конкретного лица.

Основными задачами данной работы являются определение:

– эффективности применения «речеподобных» шумовых помех по сравнению с использованием белого шума;

– минимального уровня мощности «речеподобной» помехи при котором невозможно распознать смысловую семантику говорящего при проведении операции шумоочистки.

В ходе проведённого исследования были сформированы следующие типы “речеподобной” помехи:

1. комбинированная помеха с поочерёдным изменением уровня сигнала;

2. ревербационная помеха;

3. помеха, созданная путём произвольной генерации букв русского алфавита;

4. комбинированная помеха с поочерёдным изменением тональности и мощности сигнала.

Ниже приведён алгоритм создания комбинированной “речеподобной” помехи с поочерёдным изменением тональности и мощности сигналов.

1. Запись 7 голосовых дорожек речи людей, которые зачитывали заранее подготовленный текст;

2. Удаление программным методом пауз между словами в записанных дорожках;

3. Преобразование каждой из записанных звуковых дорожек путём случайной пе-

рестановки фрагментов записи и изменение уровня сигнала этих фрагментов относительно уровня других сигналов;

4. Микширование преобразованных звуковых дорожек с добавлением дорожки белого шума;

5. Выполнение реверса суммарной речевой дорожки (одним из первых этапов при проведении операции шумоочистки является включение записи в обратном порядке). При выполнении данного этапа при попытке расшифровать запись, злоумышленник получит изменённый вариант информативного сигнала.

С помощью кроссплатформенного фреймворка Qt для формирования "речеподобного" шума, основанного на произвольной генерации букв, были проделаны следующие действия:

создание сэмплов (небольшой оцифрованный звуковой фрагмент) букв русского алфавита (рис. 2), за исключением твёрдого и мягкого знака;

разделение полученных сэмплов на 4 блока (гласные, согласные, глухие, звонкие);

выбор блоков для генерации (чередование согласных – гласных, звонких – гласных, глухих – гласных);

произвольная генерация букв (согласные – гласные).

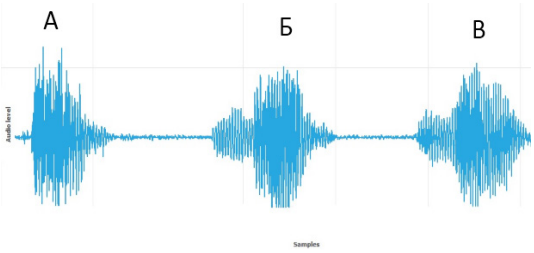

Рис. 2. Создание семплов букв русского алфавита

Вышеизложенный алгоритм является ключевым в принципиальной схеме формирования помехи (рис. 3). Основной целью генератора шума, построенного на использовании «речеподобной» помехи является не зашумление собеседника, а создание маскирующих помех в возможной точке перехвата информации.

Частотный диапазон речи лежит в пределах 70-7000 Гц. Однако около 95% энергии речевого сигнала находится в диапазоне 175-5600 Гц. Примем в качестве критерия уровень звукового давления в 60-65 дБ, который равен выступлению человека в аудитории без

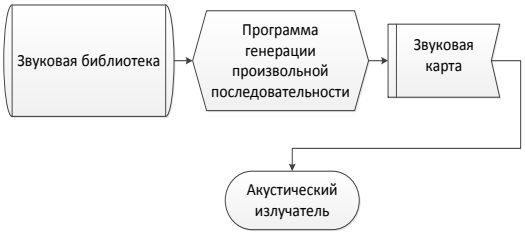

Рис. 3. Схема создания помехи

использования средств звукоусиления. Разборчивостью речи называют относительное или процентное количество принятых артикулянтами элементов речи из общего количества переданных по среде распространения.

Выделяют слоговую S, смысловую и словесную W разборчивость. Их статистическая зависимость между собой определена на графике (рис. 4).

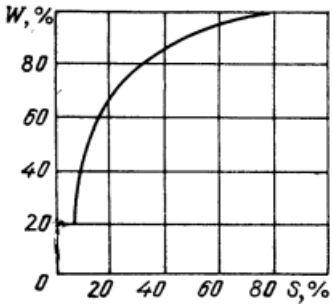

Рис. 4. Зависимость между словесной и слоговой разборчивостью речи

В таблице 1 представлен диапазон разборчивости для различных уровней понятности речи[3].

Таблица 1

Таблица словесной и слоговой разборчивости

Уровень понятности	Слоговая разборчивость W,%	Словесная разборчивость S, %
Низкий	75-87	25-40
Средний	87-93	40-56
Высокий	93-98	56-80
Очень высокий	>98	>80

На рисунках (рис. 4, 5) представлены амплитудно-частотные характеристики (АЧХ) защищаемого сигнала и "речеподобного" шума с поочерёдным изменением тонально-

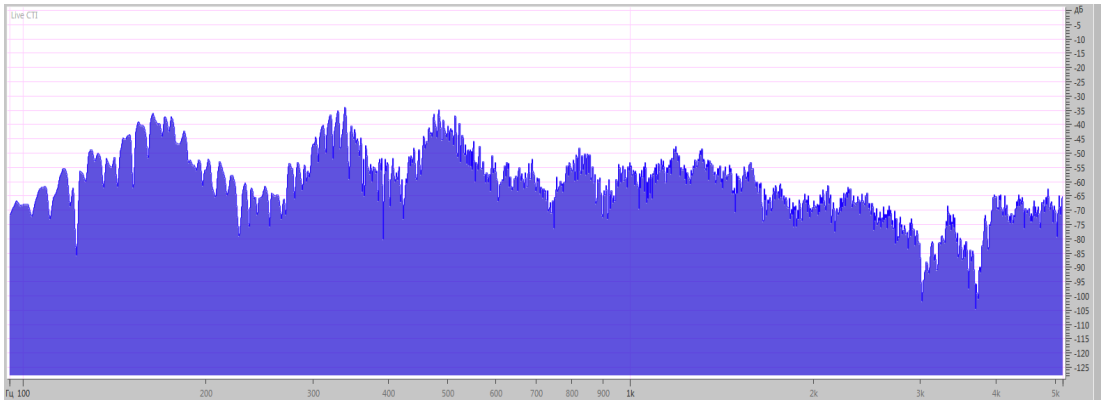

Рис. 5. АЧХ защищаемого сигнала

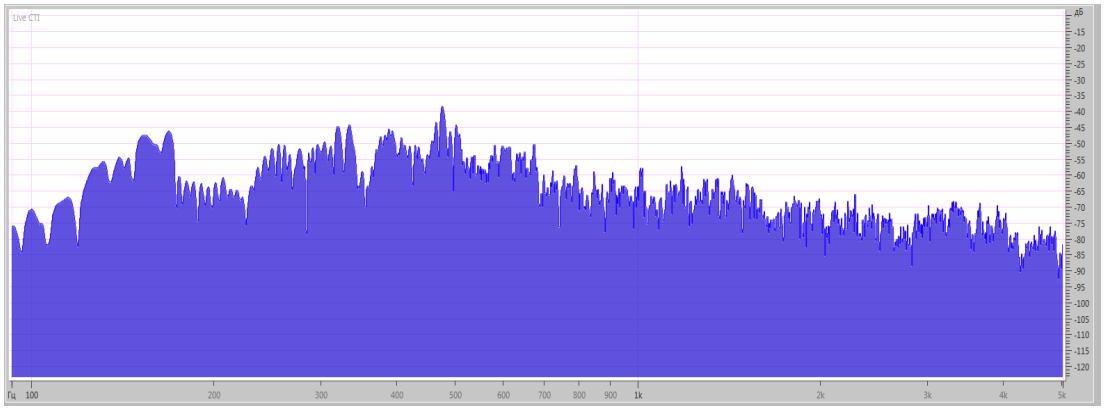

Рис. 6. АЧХ комбинированной помехи

сти, формируемого из скрываемого речевого сигнала.

На представленных спектрах можно заметить(рис. 4, 5), что данный вид помехи имеет огибающую амплитудного спектра, подобной тестовому речевому сигналу. Этот факт свидетельствует о возможности подстроить «речеподобный» шум под конкретного человека для достижения максимальной эффективности зашумления.

Определим разборчивость речи при использовании комбинированной “речеподобной” помехи с поочерёдным изменением мощности и тональности сигнала с помощью метода. В качестве площадки проведения эксперимента использовалась комната площадью 37 м^2. Ограждающие конструкции не обладали высокими звукопоглощающими свойствами. Дикторы зачитывали специальную артикуляционную таблицу в указанном помещении. Полученную в результате запись давали на прослушивание аудиторам, которые не находились в помещении во время проведении эксперимента, и записывали услышанное в протокол испытания.

Таблица 2

Артикуляционная таблица

але	бух	выр	сна	онса	ари	расо	няй
инчи	сить	сиф	аво	жей	чит	пам	зем
стро	паню	каф	ший	обла	иде	вра	жась
зым	лях	уне	нех	дись	алат	бла	вир

С помощью артикуляционной шкалы разборчивости речи (рис. 7) определялось, удалось ли выяснить содержание ведущегося в помещении разговора. Большое количество продиктованных слогов позволяет усреднить

Рис. 7. Шкала артикуляционной разборчивости речи

погрешность измерения, а использование звукосочетаний, не несущих никакой смысловой нагрузки, не даёт домыслить зашумлённую речь.

При описанном выше подходе при суммарном интегральном уровне белого шума 59 дБ словесная разборчивость составила 27% (при прослушивании записи можно сделать о самом факте наличия речи, но нельзя установить смысл слов и тематики разговора). Аналогичной словесной разборчивости удалось достичь при уровне "речеподобной" помехи 50 дБ, что свидетельствует об ее эффективности.

Для уточнения результатов, с помощью организации-лицензиата были проведены измерения и расчёт словесной разборчивости для каждой из разработанных помех. Измерения выполнялись с помощью программно-аппаратного комплекса «Спрут 7-М».

Рис. 8. Программно-аппаратный комплекс для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам «Спрут 7-М»

Контрольная точка располагалась за дверью, в месте возможной установки закладных устройств. Дверной проём не был оборудован тамбуром, уплотнителем и резиновыми проставками. Звукоизоляция проема на частоте 1000 Гц составила 33 дБ.

Интегральный уровень тестового сигнала

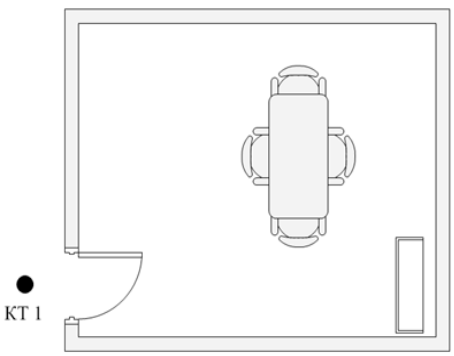

Рис. 9. Схема помещения

выбран организацией-лицензиатам равным типовой речи со средним уровнем громкости. В качестве генератора белого шума использовалась Соната – АВ.

Ниже представлена сравнительная таблица эффективности применении "речеподобных" шумовых помех по сравнению с белым шумом (табл. 3). При словесной разборчивости равной 10 % (при данном значении невозможно установить предмет ведущегося в помещении разговора даже при проведении операции шумоочистки) интегральный уровень помехи белый шум составил 69,49, тогда как "речеподобного" шума 58,75. Из рассмотренных шумовых помех наиболее эффективной оказалась комбинированная "речеподобная" помеха: поочередное изменение уровня и тональности сигнала. Белы шум оказался наиболее громким по сравнению с другими маскирующими шумовыми помехами. Из всех рассмотренных "речеподобных помех", наименее оптимальной является шум, генерируемый путём произвольной генерации букв русского алфавита.

Таблица 3

Сравнительная таблица зависимости словесной разборчивости от интегрального уровня помехи

Вид помехи	W, %	Интегральный уровень помехи
"Речеподобная" помеха с поочерёдным изменением тональности сигнала	10	58,75
"Речеподобная" помеха, созданная путём произвольной генерации букв русского алфавита	10	63,17
"Речеподобная реверберационная" помеха	10	61,09
"Речеподобная" помеха, воспроизводимая с фильтром "Инверсия"	10	60,01
Белый шум (Соната-АВ)	10	69,49

Таким образом, было экспериментально доказано, что для достижения требуемого уровня словесной разборчивости интегральный уровень белого шума следует задать на 9 дБ больше по сравнению с "речеподобной" помехой. "Речеподобная помеха" сформированная путём микширования звуковых дорожек с переменным увеличением уровня и тональности сигнала является самой эффектив-

ной из рассмотренных нами помех. Стоит отметить, что современные САЗ позволяют редактировать уровень шума в каждой октаве. Однако, даже в этой ситуации "речеподобная" САЗ при одинаковом значении словесной разборчивости будет обладать более высокими маскирующими свойствами и менее раздражающе воздействовать на нервную систему человека, по сравнению с белым шумом.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Макаров Ю.К., Хорев А.А. Методы защиты речевой информации и оценки их эффективности // Защита информации. – Конфидент.: 2001. - № 4, 22-33 с.

2. Сапожков М.А. Акустика // Справочник. – М.: Радио и связь 1998. – 186-192 с.

3. Фучко М.М., Широких А.В., Захаров А.А., Несговоров Е.С., Оленников Е.А. Аудиовыход как скрытый канал утечки данных: технологии создания и методы защиты //Вестник УрФО. Безопасность в информационной сфере. – Челябинск: Изд. Центр ЮУрГУ, 2016. - № 3(21).

References

4. Fuchko MM, Shirokih AV, Zakharov AA, Nesgovorov ES, Olennikov EA Audio output as a hidden data leakage channel: creation technologies and security methods // Vestnik URFO. Security in the information sphere. - Chelyabinsk: Izd. Center SUSU, 2016. -№ 3 (21).

5. Sapozhkov M.A. Acoustics / / Handbook. - M .: Radio and Communication 1998. - 186-192 p.

6. Makarov Yu.K., Khorev AA Methods of protection of speech information and evaluation of their effectiveness // Information protection. - Confidential: 2001. - No. 4, 22-33 c.

АСЯЕВ Григорий Дмитриевич, студент высшей школы электроники и компьютерных наук кафедры "Защита информации" Южно-Уральского Государственного Университета. Россия, 454080, г.Челябинск, проспект Ленина, д 76. E-mail: asyaev1996@mail.ru

ASYAEV Grigoriy, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

АНТЯСОВ Иван Сергеевич, руководитель, старший преподаватель кафедры "Защита информации научный " Южно-Уральского Государственного Университета. Россия, 454080, г. Челябинск, проспект Ленина, д 76. E-mail: antiasovis@susu.ru.

ASYAEV Grigoriy, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

ANTYASOV Ivan, research manager, senior teacher Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: antiasovis@susu.ru.

УДК 004.048 + 621.396.62 Вестник УрФО № 2(28) / 2018, с. 25–30

Швырев Б.А., М.В.Бердник, Гострый М.Б.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПАССИВНЫХ РАДИОЗАКЛАДОК НА ЭЛЕКТРОННЫЕ МОДУЛИ, ОБРАБАТЫВАЮЩИЕ ИНФОРМАЦИЮ

Рассматривается влияние пассивного переизлучателя на электронный модуль обработки информации, обобщенной моделью которого приняли автогенератор. Модель АГ выбрана для учета влияния и оценки совместной работы как минимум двух нелинейных элементов и двух резонансных систем. Проведенные экспериментальные исследования показывают удовлетворительную их совместную работу.

Ключевые слова: *пассивный переизлучатель, автогенератор, диод-диполь, туннельный диод.*

Shvyrev B.A., M.V.Berdnik, M.B.Gostriy

INVESTIGATION OF THE EFFECT OF PASSIVE RADIO BOOKMARKING ON ELECTRONIC MODULES THAT PROCESS INFORMATION

The influence of the passive re-radiator on the electronic information processing module is considered, the generalized model of which was taken by the self-oscillator. The AG model was chosen to take into account the influence and evaluation of the joint work of at least two non-linear elements and two resonant systems. The conducted experimental studies show satisfactory their joint work.

Keywords: *passive re-radiator, self-oscillator, diode-dipole, tunnel diode.*

Использование классического радиоканала для съема информации легко обнаруживается средствами контроля эфира и могут быть деактивированы. Альтернативным способом съема информации является пассивная радиозакладка использующая для создания информационного радиоканала падающее стороннее высокочастотное электромагнитное излучение, при этом источник излучение может быть, как непосредственный участник этой схемы съема информации и сторонним источником на разрешенном частотном диапазоне. Развитие беспроводных технологий значительно повысили плотность радиоизлучения на контролируемом помещении. Обычно пассивный переизлучатель

используется для организации акустического канала утечки.

Работоспособность пассивной переизлучающей радиозакладки для снятия информации с электронных модулей обрабатывающих информацию не тривиальна, в силу особенности ее реализации.

Рассмотрим возможность реализации указанного канала утечки. В качестве модели модуля обрабатывающего информацию рассмотрим автогенератор гармонических колебаний, как наиболее чувствительная система к нештатным подключениям устройств и электронных компонентов.

Автогенераторами (АГ) называются устройства, в которых энергия источников питания преобразуется в энергию высокочастотных колебаний без внешнего возбуждения. АГ являются первичными источниками колебаний, частота и амплитуда которых определяется только собственными параметрами схемы и должны в очень малой степени зависеть от внешних условий. В состав АГ обязательно входит активный элемент (АЭ) и колебательная система (КС). АЭ может быть двухполюсником (туннельный диод, диод Ганна и др.) или трехполюсником (транзистор, лампа), который управляет поступлением порций энергии источников питания в КС для поддержания определенной амплитуды. КС задает частоту колебаний, обычно близкую к одной из ее собственных частот.

Критерием выбора схемы АГ для анализа влияния переотражателя на электронные системы обрабатывающую информацию выбрали минимальную потребляемую схемой мощностью и минимальное напряжение питания, так как подключение дополнительной высокочастотной резонансной системы добавляет напряжение, поступающее на АГ, что может привести к искажениям работы АГ – уход частоты, в нашем случае можно трактовать как разрушение первичной информации, а так же срыв колебаний АГ, что можно трактовать как нарушение процесса обработки первичной информации электронного модуля в целом и в принципе не возможность реализации рассматриваемого канала утечки.

Существует много схем автогенераторов на различных активных элементах. К АГ на двухполюсниках относятся: АГ на туннельном диоде (ТД); АГ на лавинно-пролетном диоде (ЛПД); АГ на диоде Ганна. К автогенераторам на трехполюсниках относятся: АГ на биполярном транзисторе; АГ на полевом транзисторе; АГ на СВЧ транзисторах; АГ на лампах; АГ на клистроне; АГ на лампах бегущей волны (ЛБВ); АГ на лампах обратной волны (ЛОВ); АГ на магнетроне.

В таблице 1 приведены потребляемые мощности и напряжения питания для автогенераторов, выполненных на различных АЭ

Таблица 1

Потребляемые мощности и напряжения питания автогенераторов

Схема автогенератора	Потребляемая мощность	Напряжение питания
АГ на ТД	порядка 1 мВт	десятки мВ
АГ на ЛПД	от сотен мВт до десятков Вт	от единиц до десятков В
АГ на диодах Ганна	от десятка мВт до нескольких Вт	единицы В
АГ на биполярных транзисторах	от десятков мВт до сотен Вт	от сотен мВ до десятков В
АГ на полевых транзисторах	от десятков мВт до сотен Вт	от единиц до десятков В
АГ на СВЧ транзисторах	от десятков до сотен Вт	десятки В
АГ на лампах	от единиц Вт до сотен кВт	от сотен В до десятков кВ
АГ на клистронах маломощные	от десятка мВт до 1 Вт	десятки В
АГ на клистронах мощные	порядка 20-30 МВт	250-300 кВ
АГ на ЛБВ	от единиц мВт до сотен кВт	порядка тысячи В
АГ на ЛОВ	от одного до 150 кВт	порядка тысячи В
АГ на магнетроне	от десятков до сотен кВт	от сотен до тысячи В

Наиболее приемлемым автогенератором из вышеперечисленных является АГ на туннельном диоде. Его потребляемая мощность составляет порядка 1 мВт, напряжение питания десятки мВ.

Туннельный диод представляет собой соединение вырожденных полупроводников различной проводимости и отличается от обычного диода большой концентрацией примесей в полупроводнике $(10^{18} \div 10^{19}\ атом/см^3)$, весьма узким p-n-переходом (10^{-6} см), большой проводимостью в обратном направлении, наличием падающего участка на прямой ветви вольтамперной характеристики.

При использовании ТД в качестве автогенератора его собственная частота генерации составляет f_0=330Мгц ÷ 2,6 ГГц. При передаче тревожного извещения частота должна быть низкой (несколько кГц), поэтому необходимо использовать колебательный контур (КК) для создания низкочастотного колебания. Расчет АГ на ТД с достаточной степенью точности приведен в справочной литературе. Максимальное значение мощности, отдаваемой нелинейным элементом в контур, составляет:

$$P_{1\max} = \frac{3}{16}\Delta I \Delta U \text{ , (1)}$$

где $\Delta I = I_{\max} - I_{\min}$ и $\Delta U = U_{\min} - U_{\max}$ – величина среднего значения тока и напряжения соответственно на ВАХ туннельного диода.

В согласованном режиме мощность, отдаваемая ТД в нагрузку, составляет 50% от потребляемой автогенератором мощности.

В оптимальном по мощности режиме амплитуда стационарных колебаний равна:

$$U_{1\max} = \frac{\Delta U}{\sqrt{2}} \text{ . (2)}$$

Имеющиеся в литературе расчеты выполнены для АГ с линейной нагрузкой в виде КК. При использовании же АГ нагруженного на пассивный переизлучатель дополнительной нагрузкой автогенератора выступает полупроводниковый диод, коммутирующий полуволновый диполь. Аналитическое описание работы такой схемы, содержащей два нелинейных элемента, достаточно сложное. Также затруднительно аналитически определить место подключения диода с монотонной ВАХ к автогенератору. Поэтому выбор осуществим на основании экспериментальных измерений [7-9].

Эффективность экспериментальных исследований оценивалась по возбуждению и поддержанию колебаний и обеспечению максимальной глубины модуляции переизлученного поля.

Выберем схему подключения к автогенератору на туннельном диоде нагрузки, которой является германиевый диод-диполь. Критерием выбора является эффективность модуляции переизлучённого поля при одинаковой потребляемой мощности. Анализу подвергались три схемы включения германиевого диода-диполя, подключенного к АГ, изображенные на рисунке 2.

Экспериментальные измерения глубины модуляции переизлучённого поля для различных схем включения нагрузочного диода-диполя в схему АГ на ТД проводились на лабораторной установке, изображенной на рисунке 1.

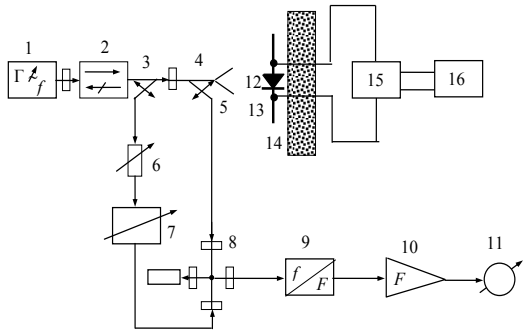

Рисунок 1 – Измерительная установка для измерения глубины модуляции переизлученного поля.

Цифрами на рисунке обозначены: 1 - генератор высокочастотных колебаний; 2 – вентиль; 3 - направленный ответвитель, создающий канал опорной волны; 4 - направленный ответвитель, отводящий сигнал в детекторную секцию; 5 – приемо-передающая антенна; 6 – аттенюатор; 7 – фазовращатель; 8 - высокочастотный сумматор; 9 – детектор; 10 – усилитель; 11 – индикатор; 12 - р-п переход; 13 - цилиндрические проводники; 14 - поглотитель высокочастотных колебаний; 15 – автогенератор; 16 - источник постоянного напряжения.

Измерения проводились на частоте F=8,4 ГГц. Эффективность модуляции оценивали по амплитуде первой гармоники рассеянного поля и сравнивали с эффективностью модуляции короткозамкнутого (КЗ) вращающегося вибратора. Глубина модуляции вращающегося диполя принята за 100%, когда вибратор параллелен вектору напряженности электрического поля E, наведенный в нем ток, а, следовательно, и амплитуда рассеянного поля максимальна; если вибратор перпендикулярен вектору E, то наведенный ток и рассеянное поле отсутствуют. Для измерений использовалась установка подобная своей измерительной частью изображенной на рисунок 2. Отличие состоит в использовании вместо диода со схемой питания КЗ вибратора прикрепленного к диэлектрическому стержню, вращающемуся вдоль оси проходящей через центр вибратора и параллельно волновому вектору k. Вращение осуществлялось электродвигателем с частотой $F_{вр}$=2кГц. Установки параметров схемы измерений в про-

цессе выполнения эксперимента оставались постоянными. Величина напряжения $U_{изм}$, фиксируемого измерителем 11, при вращающемся КЗ вибраторе была принята за 100%. Значения, полученные при использовании различных схем, сравнивались с опорной величиной. Полученные результаты представлены в таблице 2.

Таблица 2

Сравнение полученных результатов с опорной величиной

Схема включения	Uизм, мВ	Pnom, мВт	M, %
КЗ вибратор	12	-	100
Параллельный. КК	2	0,165	16
Последовательный. КК	0,5	0,165	4
Цепь	0,25	0,165	2

Из таблицы 2 следует, что при различных вариантах подключения диода-диполя потребляемая автогенератором мощность остается постоянной. Наибольшая эффективность модуляции рассеянного поля получена при включении управляющего диода по схеме параллельно КК (рисунок 3.а). Эффективность модуляции составила 16% от опорного значения.

Проанализировав схемы включения нагрузочного диода в автогенератор, выберем схему включения диода параллельно КК (рисунок 3.а). выполним для данной схемы расчет.

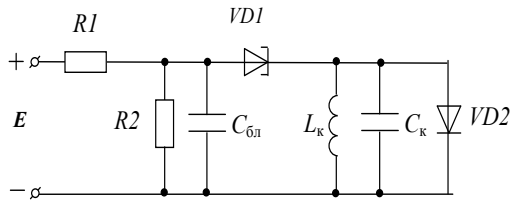

Рисунок 2 (а) – Схема подключения диода-диполя к АГ на ТД параллельно КК.

Буквами на рисунках обозначены: *E* - источник питания постоянного тока, *R1* и *R2* - резисторы, задающие режим работы ТД по постоянному току, $C_{бл}$- блокировочный конденсатор в цепи питания, *VD1* - туннельный диод, $L_к$ и $C_к$ - индуктивность и емкость колебательного контура, VD2 - нагрузочный германиевый диод.

Рассмотрим возможные устойчивые режимы работы автогенератора, для этого вос-

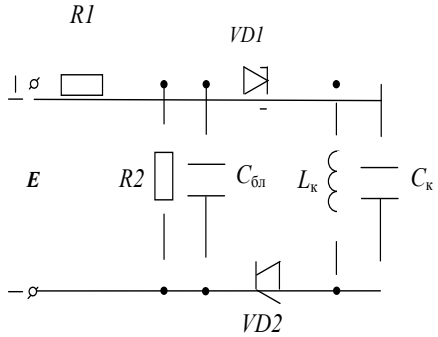

Рисунок 2 (б) – Схема подключения диода-диполя к АГ на ТД последовательно КК.

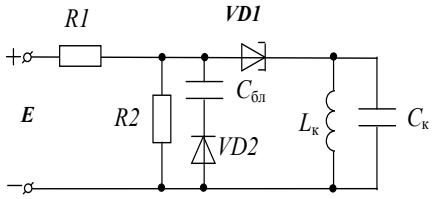

Рисунок 2 (в) – Схема подключения диода-диполя к АГ на ТД в цепь блокировочного конденсатора.

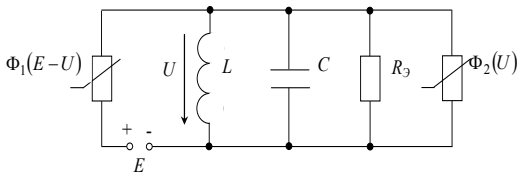

Рисунок 3 – Эквивалентная схема с двумя нелинейными элементами.

пользуемся эквивалентной схемой, изображенной на рисунке 4. Схема содержит два нелинейных элемента: туннельный диод с вольтамперной характеристикой $Ф_1$(u), нелинейную нагрузку колебательного контура, в качестве которой будем понимать полупроводниковый диод с вольтамперной характеристикой $Ф_2$(u). ВАХ ТД аппроксимируем полиномиальной аппроксимацией:

$$i = a_1 u + a_3 u^3, \quad (3)$$

где $a_1 = -\frac{3}{2}\frac{\Delta I}{\Delta U}$, $a_3 = 2\frac{\Delta I}{(\Delta U)^2}$.

Определим вид аппроксимации диода нагрузки исходя из условия обеспечения максимальной точности оценки, простоты математических расчетов. Максимальная точность аппроксимации ВАХ полупроводникового диода является экспоненциальная аппроксимация вида:

$$i = I_0\left(\exp(\beta u) - 1\right), \quad (4)$$

где I_0 - ток ветви отрицательного смещения полупроводникового диода, β - коэффи-

циент, определяющий скорость изменения тока.

Данный вид аппроксимации сложен в аналитических расчетах. Наиболее простой вид аппроксимации, дающий грубое приближение является кусочно-линейная аппроксимация вида:

$$i = \begin{cases} 0; & u \le U \\ S(u-U); & u \ge U \end{cases}; \quad (5)$$

Для проведения анализа устойчивости составим дифференциальное уравнение (5), описывающее работу АГ по эквивалентной схеме (рисунке 4):

$$C\frac{du}{dt} + \frac{u}{R_э} + \frac{1}{L}\int u\,dt + \Phi_2(u) = \Phi_1(E-u), \quad (6)$$

где u - падение напряжения на КК.

Принимая падение на ТД равным u, выражение (6) можно переписать в виде:

$$C\frac{d(E-u)}{dt} + \frac{(E-u)}{R_э} + \frac{1}{L}\int (E-u)dt + \Phi_2(E-u) = \Phi_1(u). \quad (7)$$

Решение общего нелинейного дифференциального уравнения второго порядка (7), позволяет выявить все особенности АГ: условия самовозбуждения, форму, частоту и амплитуду (мощность) колебаний, устойчивость стационарных режимов и т.п. Однако численное решение нелинейного дифференциального уравнения второго порядка затруднительно из-за сложного переходного режима. Определим возможные состояния равновесия системы по нагрузочным характеристикам.

На рисунке 5 представлены ВАХ туннельного диода $\Phi_1(u)$ и нагрузочная характеристика, складывающаяся из ВАХ диода и прямой нагрузочной характеристики эквивалентного сопротивления контура $\frac{(E-u)}{R_э} + a_2(E-u)^2$. ВАХ ТД и нагрузочная характеристика для постоянного тока в общем случае имеют три точки пересечения (А, В и С), соответствующие трем возможным состояниям равновесия.

Определим максимальное значение

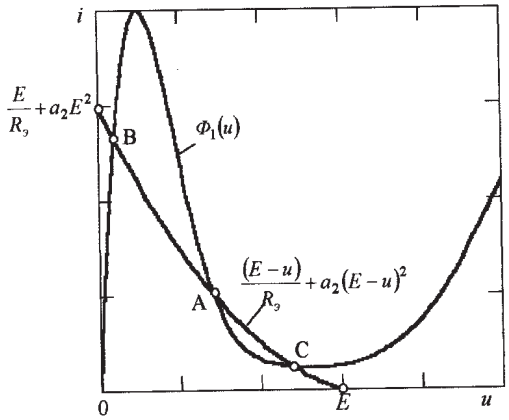

Рисунок 5 – Графическое определение состояний равновесия системы.

мощности, отдаваемой нелинейным элементом в контур для конкретного туннельного диода АИ101А. Данный тип диода определен по справочнику исходя из условий минимальных значений ΔI и ΔU. Используя формулу (2.12), полученная мощность в нагрузке, отдаваемая ТД на первой гармонике составила P_{1max}=*0,0464мВт*. Тогда в согласованном режиме мощность, потребляемая АГ от источника питания составит: $P_{пот}=2P_{1max}$=0,0928мВт. Сравнивая полученный результат с экспериментальными значениями (таблица 2) получаем различие приблизительно в два раза. Это объясняется разбросом параметров элементов схемы АГ.

Как показали проведенные расчеты и экспериментальные исследования получение максимальной мощности и удовлетворение условий устойчивости по постоянному и переменному току удовлетворяются. Нелинейный элемент расширяет спектр поданного на него гармонического сигнала, что в свою очередь приводит к перераспределению мощности по гармоникам.

Проведенные измерения показали, что включение полупроводникового диода параллельно колебательному контуру АГ на туннельном (рисунок 3) не ухудшает эффективности работы последнего.

Таким образом определен канал утечки информации по пассивной радиозакладке подключенной к электронному модулю, обрабатывающему информацию.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская, д.2. E-mail: bor2275@yandex.ru

БЕРДНИК Мария Викторовна, доцент кафедры компьютерных технологий и информационной безопасности. Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская, д.2. E-mail: marviktr@mail.ru

ГОСТРЫЙ Максим Борисович, студент кафедры компьютерных технологий и информационной безопасности, Кубанский государственный технологический университет. 350000 г. Краснодар, ул. Московская, д. 2. E-mail: maxim.gostriy@gmail.com

SHVYREV Boris, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2 Moskovskaya street. E-mail: bor2275@yandex.ru

MARIA Berdnik, Associate Professor of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2 Moskovskaya street. E-mail: marviktr@mail.ru

MAXIM Gostriy, Student of the Department of Computer Technologies and Information Security. Kuban State Technological University. 350000 Krasnodar, Bld. 2 Moskovskaya street. E-mail: maxim.gostriy@gmail.com

УДК 004.056.2 + 002.004.056 Вестник УрФО № 2(28) / 2018, с. 31–35

Соколов С. С., Новоселов Р. Ю., Митрофанова А. В.

МЕТОДЫ ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ ИНФОРМАЦИИ В ВЫСОКОНАГРУЖЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье рассматривается проблема доступности информации в современном мире в высоконагруженных информационных системах. Рассмотрены основные понятия, такие как - распределенная вычислительная система, высоконагруженная информационная система, big data. Приведены критерии распределенной вычислительной системы. Также описаны основные методы управления нагрузкой и повышения отказоустойчивости высоконагруженных информационных систем, их преимущества и недостатки, в частности баз данных. Приводится пример реализации одного из методов.

Ключевые слова: *высоконагруженные информационные системы, распределенные вычислительные системы, базы данных, доступность информации, методы оптимизации нагрузки.*

Sokolov S. S., Novoselov R. Y., Mitrofanova A. V.

METHODS TO ENSURE THE AVAILABILITY OF INFORMATION IN HIGHLOAD INFORMATION SYSTEM

The article analyses problem of information availability in modern world in highload information systems. Described main concepts, such as distributed computer system, highload information system, big data. Gave criteria of distributed computer system. Also considered main methods of load managing and increasing resilience of highload systems, its advantages and disadvantages, particularly databases. Gave an example of realization one of methods.

Keywords: *highload information system, distributed computer system, databases, information availability, methods of load managing.*

Введение

В современном мире количество информации неуклонно растет. Существует проблема, которая называется "информационный взрыв" - постоянное увеличение скорости и объемов публикаций (объёма информации) в масштабах планеты. Как известно, главными свойствами данных является конфиденциальность, целостность и доступность.[1] В силу глобализации мира, развития интернета, повышения требований к скорости, появляется множество задач, связанных с обеспечение доступности информации. Современные информационные системы в качестве основной характеристики имеют распределенную архитектуру, но даже распределенная система не спасает от нагрузки, как следствие, от проблем доступа, а соответственно, не может обеспечить часть или все требования к информации. Существуют различные методы обеспечения доступности. В данной статье будет дано определение высоконагруженной информационной системе, а также будут рассмотрены способы оптимизации нагрузки.

Определение понятий и постановка задачи

Для обсуждения данной проблемы нужно дать определение высоконагруженной ИС, но сначала поговорим о распределенной вычислительной системе.

Эндрю Таненбаум , в своем фундаментальном труде «Распределенные системы. Принципы и парадигмы»[2] предложил следующее определение:

«**Распределенная вычислительная система** – это набор соединенных каналами связи независимых компьютеров, которые с точки зрения пользователя некоторого программного обеспечения выглядят единым целым».

Выделяют следующие важные характеристики РВС:

– возможность работы с различными типами устройств: с различными поставщиками устройств, с различными операционными системами, с различными аппаратными платформами;

– возможность простого расширения и масштабирования;

– перманентная (постоянная) доступность ресурсов (даже если некоторые элементы РВС некоторое время могут находиться вне доступа);

– сокрытие особенностей коммуникации от пользователей.

Вычислительные среды, состоящие из множества вычислительных систем на базе разных программно-аппаратных платформ, называются *гетерогенными*.

Для того чтобы РВС могла быть представлена пользователю как единая система, применяют следующие типы прозрачности в РВС:

– *прозрачный доступ к ресурсам* – от пользователей должна быть скрыта разница в представлении данных и в способах доступа к ресурсам РВС;

– *прозрачное местоположение ресурсов* – место физического расположения требуемого ресурса должно быть несущественно для пользователя;

– *репликация* – сокрытие от пользователя того, что в реальности существует более одной копии используемых ресурсов;

– *параллельный доступ* – возможность совместного (одновременного) использования одного и того же ресурса различными пользователями независимо друг от друга. При этом факт совместного использования ресурса должен оставаться скрытым от пользователя;

– *прозрачность отказов* – отказ (отключение) каких-либо ресурсов РВС не должен оказывать влияния на работу пользователя и его приложения.

Как мы видим, многие описанные выше тезисы характерны и для систем, которые мы называем высоконагруженными. Но чтобы выяснить, что из этого является классом и подклассом, мы попробуем дать определение высоконагруженной ИС.

Высоконагруженная ВС - *это распределенная ВС,* к которой при проектировании и разработке применяются соответствующие техники не только распределенных систем, а также другие, например: определенные шаблоны при проектировании базы данных, алгоритмика и др.

Также понятие высоконагруженной ВС может быть (но не обязательно) связано с понятием больших данных (*big data*). Не будем углубляться в большие данные, лишь дадим определение и примеры использования, чтобы читатель мог понять, как связана тема статьи и big data.

Большие данные (англ. big data) — серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения воспринимаемых человеком результатов, эф-

фективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся в конце 2000-х годов, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence.

То есть, как ни странно **big data** - это не объем данных, а методы работы с ними.

Примеры задач, в которых используется big data:

– Логи поведения пользователей в интернете.

– GPS-сигналы от автомобилей для транспортной компании.

– Данные, снимаемые с датчиков в большом адронном коллайдере.

– Оцифрованные книги в Российской Государственной Библиотеке.

– Информация о транзакциях всех клиентов банка.

– Информация о всех покупках в крупной ритейл сети и т.д.

Такие данные скорее всего хранятся в базе данных, или в простых текстовых файлах, что реже (напр. логи поведения пользователей в интернете). В рамках данной статьи под высоконагруженной системой мы будем рассматривать web-приложение.

Таким образом, в рамках статьи мы будем решать задачу снижения нагрузки на информационную систему, и в первую очередь на базу данных.

Способы решения задачи

В предыдущей работе[3] было доказано, что скорость работы базы данных напрямую зависит от количества данных, содержащихся в ней. Поэтому скорее всего первое, что будет тормозить систему, это база данных. Необходимо выделить ее на отдельный сервер, подобные действия позволят увеличить ее производительность и снизить ее негативное влияние на остальные компоненты (вычислительные ресурсы, веб-сервер и др.). Далее, выносим веб-сервер на отдельный узел. Освободим больше ресурсов для вычисления. После можно разделить вычисления на несколько серверов, подключить кэширование, очереди, балансировщики. Но обычно самым тяжелым элементом системы является база данных, поэтому оптимизации данного узла необходимо уделить гораздо больше внимания. Масштабирование баз данных - это одна из самых сложных задач во время роста ИС. Существует очень много практик — денормализация, репликации, шардинг и многие другие. Рассмотрим основные:

Денормализация данных

Существует так называемая нормальная форма хранения данных, которая предполагает избегания дублирования данных. Ключевых правила два:

– **Атомарность** означает, что все сущности хранятся в неделимом виде. Например, если мы храним адрес, то он скорее всего будет поделен на название города, страны и улицу. Все они должны быть представлены отдельными таблицами. Название города будет атомарным, т.к. дальше делиться не будет.

– **Уникальность** требует, чтобы каждая сущность была определена только один раз. Например, название города с идентификатором 1 должно присутствовать только в таблице *cities*.

Денормализация — это постепенный процесс избавления от правил нормализации там, где это необходимо. Обычно это случаи, в которых есть частые повторные запросы к логически связанным данным.[4]

Простым примером является хранение названия города вместе с данными пользователя. Если денормализировать эти данные, то можно будет получить название города одним SQL запросом, а не двумя. Далее в рамках статьи мы рассмотрим пример денормализации данных.

Репликация данных

Репликация — одна из техник масштабирования баз данных. Состоит эта техника в том, что данные с одного сервера базы данных постоянно копируются (реплицируются) на один или несколько других (называемые репликами). Таким образом появляется возможность распределить нагрузку с одного сервера на несколько.

Существует два основных подхода при работе с репликацией данных:

– Репликация Master-Slave;

– Репликация Master-Master.[5]

Помимо повышения производительности, есть несколько причин для использования репликаций:

– Отказоустойчивость - если Slave сервер откажет, можно без проблем перевести все запросы на чтение на другие сервера. Если откажет Master, можно перевести запросы записи на реплики, и когда Master восстановит свою работу, он сможет перенять на себя роль Slave сервера;

– Резервирование данных - на какое-то

время в случае, например, оптимизации таблицы, можно остановить сервер и ничего страшного не случится;

– Отложенные вычисления - если в очереди есть сложный запрос, для его выполнения можно использовать Slave сервер, чтобы не замораживать работу всей системы.

Также, в силу того, что на Slave сервера передаются не сами данные, а запросы на их изменения, можно использовать разные схемы, типы таблиц или индексы.

Шардинг

Шардинг — это принцип масштабирования базы данных, когда данные разделяются по разным серверам. В нашем распоряжении есть два подхода:

Вертикальный шардинг - это простое распределение таблиц по серверам. Например, вы помещаете таблицу users на одном сервере, а таблицу orders на другом. В этом случае, группы таблиц, по которым выполняются JOIN, должны находится на одном сервере.

Горизонтальный шардинг - разделение очень больших таблиц, которые перестают помещаться на одном сервере, на разные сервера. Это сильно усложняет логику приложения, однако на данный момент не существует лучших механизмов масштабирования.[5]

Лучшим вариантом, по мнению автора статьи совмещение всех этих методов. Денормализация данных поможет избавиться от сложных JOIN запросов - соединение нескольких таблиц является очень ресурсоемкой операцией. Реплики, как было сказано выше, помогут распределить нагрузку с одного сервера на несколько. Ну и как самый эффективный метод, шардинг позволит получить действительно оптимизированную и быструю высоконагруженную систему.

Пример оптимизации базы данных

Для примера разберем некоторую социальную сеть. Мы заполнили таблицу тестовыми данным - 10000 пользователей и 5 городов. Примеры таблиц представлены ниже. Время выполнения запросов измерялось с помощью встроенного профайлера MySQL.

Предположим, что необходимо выбрать пользователя с ID 6, включая город пользователя. С учетом текущей схемы базы данных необходимо использовать JOIN. Запрос будет выглядеть следующим образом:

*SELECT *,`name` AS `city_name` FROM `users` LEFT JOIN `cities` ON `users`.`city_id`=`cities`.`id` WHERE `users`.`id`=6*

Таблица 1

Часть таблицы users

ID	firstname	lastname	city_id
1	Jonh	Smith	2
2	Anthony	Park	3
3	Richard	Edwards	1
4	Reynard	McKinney	2
5	Charles	Turner	1

Таблица 2

Часть таблицы cities

ID	name
1	London
2	New-York
3	Paris

Данный запрос занимает 0.000502 секунды. Теперь попробуем денормализовать данные: добавим столбец ‘city_name’ в таблицу ‘users’, куда запишем название города.

Добавляем поле:

ALTER TABLE `users` ADD COLUMN `city_name` VARCHAR(100);

Теперь для того, чтобы получить информацию о пользователе, включая его город, необходимо выполнить простой запрос:

*SELECT * FROM `users` WHERE `id`=6;*

Данный запрос занимает 0.000398 секунды. Соответственно, прирост производительности более чем на 20%. А в случае с большим объемом данных[3], результат будет гораздо лучше.

Заключение

Задача с доступностью данных с ростом ИТ становится все актуальнее, и как показано в статье. Современный мир отличается глобализацией, когда информация и люди, которым она требуется, находятся в разных уголках земного шара. С помощью методов, описанных в данной статье, возможно обеспечить информацию необходимым набором свойств.

Самым простым способом оптимизации является денормализация данных. Однако, такое решение конечно - невозможно денормализировать данные бесконечно. Репликация и шардинг являются более востребованными способами оптимизации, к тому же могут применяться вместе. Но стоит отметить, что ни один из представленных способов не является панацеей, и на этапе проектирования системы необходимо использовать все способы в комплексе, для достижения наилучшего результата.

Литература

1. ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации. Основные термины и определения // Защита информации. Москва: Стандартинформ, 2008.

2. Таненбаум Э. Распределенные системы. Принципы и парадигмы. - СПб:Питер, 2003.

3. Новоселов Р.Ю., Соколов С.С. Тестирование и анализ скорости двух популярных реляционных баз данных при различных нагрузках // Материалы работы науч.-исслед. конф. студентов и аспирантов ф-та информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА — 2016» 11 декабря 2015 г./ Спб.: Изд-во ГУМРФ им. Адмирала С. О. Макарова, 2016

4. Денормализация данных [Электронный ресурс] // HighLoad++; URL: https://ruhighload.com/post/Денормализация+данных (дата обращения: 24.01.2018)

5. Репликация данных [Электронный ресурс] // HighLoad++; URL: https://ruhighload.com/post/Репликация+данных (дата обращения: 12.01.2018)

6. 5 стратегий работы с высокими нагрузками в MySQL [Электронный ресурс] // HighLoad++; URL: https://ruhighload.com/post/4+стратегии+работы+с+высокими+нагрузками+в+MySQL (дата обращения: 17.12.2017)

References

1. GOST R 53114-2008. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya // Zashchita informatsii. Moskva: Standartinform, 2008.

2. Tanenbaum E. Raspredelennyye sistemy. Printsipy i paradigmy. - SPb:Piter, 2003.

3. Novoselov R.YU., Sokolov S.S. Testirovaniye i analiz skorosti dvukh populyarnykh relyatsionnykh baz dannykh pri razlichnykh nagruzkakh // Materialy raboty nauch.-issled. konf. studentov i aspirantov f-ta informatsionnykh tekhnologiy. «IT: VCHERA, SEGODNYA, ZAVTRA — 2016» 11 dekabrya 2015 g./ Spb.: Izd-vo GUMRF im. Admirala S. O. Makarova, 2016.

4. Denormalizatsiya dannykh [Elektronnyy resurs] // HighLoad++; URL: https://ruhighload.com/post/Denormalizatsiya+dannykh (data obrashcheniya: 24.01.2018).

5. Replikatsiya dannykh [Elektronnyy resurs] // HighLoad++; URL: https://ruhighload.com/post/Replikatsiya+dannykh (data obrashcheniya: 12.01.2018).

6. 5 strategiy raboty s vysokimi nagruzkami v MySQL [Elektronnyy resurs] // HighLoad++; URL: https://ruhighload.com/post/4+strategii+raboty+s+vysokimi+nagruzkami+v+MySQL (data obrashcheniya: 17.12.2017).

СОКОЛОВ Сергей Сергеевич, заведующий кафедрой «Комплексное обеспечение информационной безопасности», Государственный университет Морского и речного флота имени адмирала С.О. Макарова, 198035, г. Санкт-Петербург, ул. Двинская, д.5/7. E-mail: sokolovss@gumrf.ru

НОВОСЕЛОВ Роман Юрьевич, аспирант, Государственный университет Морского и речного флота имени адмирала С.О. Макарова, 198035, г. Санкт-Петербург, ул.Двинская, д.5/7. E-mail: rnovoselov93@gmail.com.

МИТРОФАНОВА Анастасия Витальевна, аспирант, Государственный университет Морского и речного флота имени адмирала С.О. Макарова, 198035, г.Санкт-Петербург, ул.Двинская, д.5/7. E-mail: mitrofanovaav@gumrf.ru

SOKOLOV Sergey, chef of department “Complex providing information security”, Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya str, Saint-Petersburg, 198035. E-mail: sokolovss@gumrf.ru

NOVOSELOV Roman, graduate student, Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya str, Saint-Petersburg, 198035. E-mail: rnovoselov93@gmail.com

MITROFANOVA Anastasya, graduate student, Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya str, Saint-Petersburg, 198035. E-mail: mitrofanovaav@gumrf.ru

УДК 004.056 + 002:004.056 Вестник УрФО № 2(28) / 2018, с. 36–42

Кляус Т. К., Наумов А. Д., Гатчин Ю. А., Бондаренко И. Б.

СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ДЕРЕВЬЕВ АТАК-КОНТРМЕР И МЕТОДА КУСТА СОБЫТИЙ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Автоматизация различных процессов на предприятиях и в организациях и постоянное усложнение архитектуры информационных систем (ИС) являются предпосылками к появлению уязвимостей ИС, которые могут быть использованы злоумышленниками для реализации угроз безопасности информации. В настоящее время существует большое количество подходов к анализу и оценке угроз и рисков, характерных для ИС. В данной статье рассмотрены деревья атак-контрмер и метод куста событий – два графических подхода к оценке безопасности ИС, позволяющих в наглядном виде представить потенциальные атаки на систему и способы противодействия им. Приведен пример построения дерева атак-контрмер и куста событий для DDoS-атак, направленных на насыщение полосы пропускания ИС. Сформулированы критерии сравнения данных двух методов и на их основании проведен анализ применимости деревьев атак-контрмер и метода куста событий для оценки безопасности ИС.

Ключевые слова: *информационная система, информационная безопасность, деревья атак-контрмер, метод куста событий, оценка защищенности информационных систем.*

Klyaus T. K., Naumov A. D., Gatchin Yu. A., Bondarenko I. B.

A COMPARATIVE STUDY OF ATTACK-DEFENSE TREES AND EVENT BUSH METHOD APPLICABILITY FOR INFORMATION SYSTEMS SECURITY ASSESSMENT

Automation of various processes at the enterprises and the area organizations and constant information systems architecture complication are the prerequisites for appearance of security vulnerabilities that can be exploited by adversaries. There is a great number of security threats and risks analysis and assessment approaches. In this article attack-defense trees and event bush method are considered. These methods are graphical security assessment approaches, allowing to describe potential attacks on the system and countermeasures to them. An example of attack-defense tree and event bush for DDoS attacks directed at information systems bandwidth saturation is given. The criteria for attack-defense trees and event bush method comparison are formulated. In accordance with the proposed criteria, the analysis of attack-defense trees and event bush method applicability in information systems security assessment is made.

Keywords: *information security, information system, attack-defense tree, event bush method, information systems security assessment.*

Информационная система (далее – ИС) представляет собой интегрированный набор компонентов для сбора, хранения и обработки данных и для предоставления информации, знаний и цифровых продуктов. Использование ИС позволило автоматизировать и ускорить решение различного рода задач, а информация и знания стали жизненно важными экономическими ресурсами. Внедрение информационных технологий постоянно открывают не только новые возможности, но и создают основу потенциальным угрозам. Развитие информационных и коммуникационных технологий привело к тому, что ИС находят все более широкое применение и в Российской Федерации. На федеральном уровне подготовлен ряд нормативно-правовых актов, регламентирующих вопросы использования данных технологий в органах государственной власти и органах местного самоуправления. Соответствующими органами разработаны методические рекомендации по предотвращению угроз ИС. Но, ввиду того, что в системном плане ИС представляет собой сложную организационно-техническую систему, характеризующуюся большим количеством разнородных параметров, становится актуальной задача анализа защищенности той или иной системы.

Защищенность информационных систем

В настоящее время вопросам оценки защищенности ИС посвящено большое количество отечественных и зарубежных публикаций. На этапе проектирования перспективным направлением в оценке защищенности ИС является представление возможностей нарушителей в виде деревьев и графов атак и вычисления на основе данного представления разнообразных метрик защищенности [1]. Деревья атак тесно связаны с графами атак, однако различие лежит в представлении состояний и действий. Центральная тема для исследований графов атак – последовательность событий [2]. Также могут применяться и иные графические подходы к моделированию возможных атак и угроз – с помощью сетей Байеса, сетей Петри, иерархиче-

ских моделей представления атак, а также с помощью метода куста событий.

Метод куста событий

Метод куста событий (англ. event bush), предложенный и разработанный [3] для того, чтобы показать поведение информации в динамических системах, находит все большее распространение и применение в различных областях наук [4]. В настоящее время метод составляет основу методологии инженерии динамических знаний и используется для разработки ее единой грамматики. Информационная модель предметной области описывается кустом событий как совокупность событий четырех типов, расположенных в определенном порядке и связанных специальными причинно-следственными связями (определяется как многопоточная структура – см. рис. 1), удовлетворяющих определенным условиям. В текстовой форме куст событий — это список определенных простых и сложных высказываний, но в отличие от метода ориентированных графов с применением прямых, косвенных, положительных и отрицательных связей узлы куста событий обозначают высказывания, а ребра (стрелки) – отношения между высказываниями, которые отражают отношения «причина – следствие» между сущностями, которые эти высказывания описывают.

Метод куста событий является перспективным методом описания динамических систем, обладающий логико-семантической строгостью. С помощью метода куста событий могут быть эффективно решены задачи описания всех возможных сценариев в рамках рассматриваемой системы; построения вероятностных моделей; накопления, обработки и хранения знаний; в т.ч. поиск скрытых взаимосвязей.

Деревья-атак контрмер

Понятие деревьев-атак контрмер (англ. attack-defense trees) впервые было введено в работе [5] и впоследствии получило широкое применение в качестве инструмента анализа сценариев атак на ИС. Деревья атак-контрмер представляют собой графический способ отображения взаимодействия между злоумышленником, атакующим ИС, и ее защитником, и позволяют изучить возможные способы атаки системы и необходимые механизмы для противодействия им. Данный подход устраняет ряд ограничений, которыми обладают деревья атак — в частности, позволяет рассмотреть сценарий чередования действий атакующего и защитника системы [6].

Дерево атак-контрмер представляет собой связный граф, не содержащий циклов и кратных ребер. Дерево атак-контрмер содержит узлы двух типов – узлы атак и узлы контрмер. Вершина дерева (корневой узел) обозначает конечную цель атакующего. Вершины, соединенные ребрами с корнем дерева, представляют собой действия злоумышленника, которые он предпринимает для достижения поставленной цели. Конечная вершина, из которой не выходит ни одного нового ребра, называется также листовым узлом или базовым действием (basic action) и представляет собой действие злоумышленника или защитную меру, которые не могут быть разложены на составляющие. Вершины, не являющиеся листовыми узлами или корнем, называются узлами ветвления. Узлы ветвления обозначаются как узлы «И» или «ИЛИ». Для того, чтобы действие узла «И» выполнялось, все исходящие из него вершины должны быть истинными – должно выполняться каждое действие из всей совокупности дочерних элементов узла ветвления. Истинное состояние узла «ИЛИ» достигается в случае, если хотя бы один из его дочерних элементов принимает истинное значение. Каждый узел, обозначающий действие злоумышленника, может иметь один дочерний узел противопо-

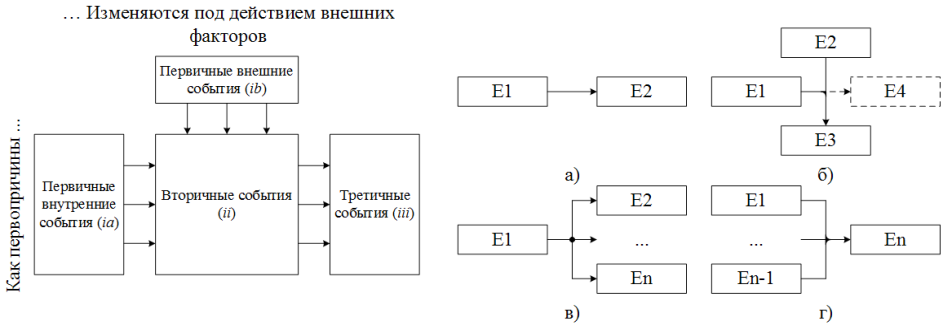

Рис. 1. Синтаксис базового блока куста событий и его соединительные элементы: поток (а), приток (б), разветвление (в) и слияние (г)

ложного типа – контрмеру. Узел контрмеры, в свою очередь, может иметь несколько уточняющих дочерних узлов и один дочерний узел, противопоставляемый защите [5].

Пример дерева атак-контрмер, построенного в программе ADTool 1.4, изображен на рис.2.

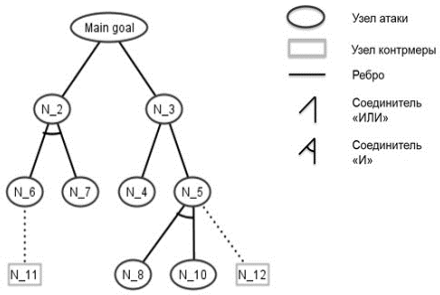

Рис. 2. Дерево атак-контрмер, построенное в программе ADTool 1.4

Построение дерева атак-контрмер и куста событий для анализа DDoS-атак, направленных на насыщение полосы пропускания ИС, и соответствующих мер их предотвращения

В данном разделе на рис. 3 и рис. 4 в форме дерева атак-контрмер и в форме куста событий представлены DDoS-атаки, использующие протоколы HTTP, ICMP, UDP, TCP, направленные на насыщение полосы пропускания, и соответствующие им контрмеры.

Для моделирования и анализа сценариев атак и защитных мер предназначен инструмент ADTool [7]. Данный инструмент позволяет создавать и редактировать деревья атак-контрмер, осуществлять расчет атрибутов дерева с помощью метода восходящего анализа, ранжировать атаки для определенных областей значений атрибутов и т.д. Кроме того, ADTool подходит для автоматизации и исследования всех разновидностей формализмов деревьев атак.

В данный момент времени метод куста событий не имеет конечного решения системы автоматизированного проектирования, однако, научными коллективами [8] активно разрабатывается интегрированная инженерная среда, позволяющая эффективно применять метод куста событий для решения широкого спектра задач научно-прикладного характера, среда, позволяющая применять метод в произвольных предметных областях, особенно таких, которые подразумевают обработку больших объемов информации и требуют серьезных вычислительных мощностей.

2. Наличие атрибутов, элементов присваивания и возможности построения пути от одного узла к другому.

Поскольку дерево атак-контрмер представляет собой связный граф, не содержащий циклов и кратных ребер, путь между узлами представляет собой последовательность вершин, в которой каждая вершина соединена со следующей ребром, причем между парами вершин имеется только по одному пути. Моделирование шагов атаки с применением циклов возможно при использовании графов атак.

В отличие от деревьев, где путь может быть только один (от одного узла к другому) — у куста событий путь между узлами можно пройти разными путями.

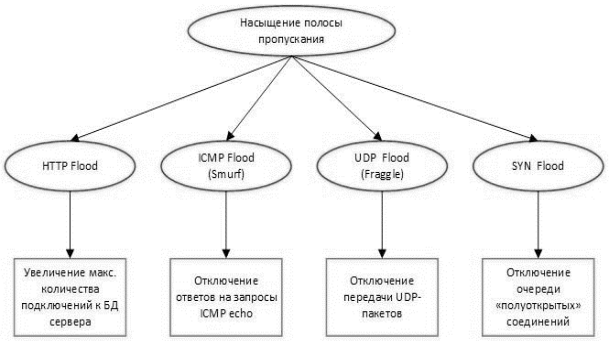

Рис. 3. DDoS-атаки и контрмеры в форме дерева атак-контрмер

Применимость деревьев атак-контрмер и метода куста событий для оценки безопасности информационных систем

В рамках данной статьи рассмотрена применимость деревьев атак-контрмер, как метода анализа ИС, по сравнению с методом куста событий.

Сравним особенности построения дерева атак-контрмер и куста событий для оценки безопасности ИС по следующим критериям:

1. Наличие или отсутствие систем автоматизированного проектирования для каждого из методов.

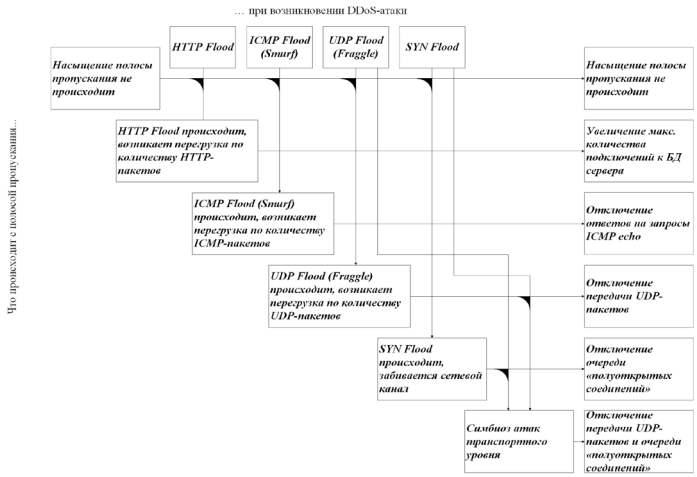

Рис. 4. DDoS-атаки и контрмеры в форме куста событий

3. Допустимость применения математического аппарата для каждого из методов.

Математический аппарат деревьев атак-контрмер был разработан в статье [5] для создания программного инструмента, позволяющего рассчитывать присваиваемые значения атрибутов листовым узлам деревьев атак-контрмер. Типы значений атрибутов зависят непосредственно от их содержания и могут принимать булевы значения, значения номинальной шкалы (низкий, средний, высокий), вещественные числа, а также дискретные и непрерывные распределения вероятностей [9].

Что касается математического аппарата, то стоит отметить то, что куст событий — вероятностная модель, представляющая собой множество событий и связей между ними и, следовательно, куст событий может быть использован для того, чтобы, например, вычислить вероятности неисправностей узлов аппаратуры по наличию или отсутствию ряда признаков основываясь на априори известных зависимостях между неисправностями и их проявлениями.

Заключение

Для подведения итогов необходимо разъяснить практический интерес описанной ранее модели, а также перспективы ее применения. Рассматриваемая модель, раскладывающая процесс DDoS-атак, направленных на насыщение полосы пропускания ИС, на минимально возможные единицы – простейшие действия, облегчает выявление потенциальных угроз развития событий на всех этапах этого процесса. Таким образом, ответственное должностное лицо за обеспечение безопасности ИС может проследить и заблаговременно выявить возможные потенциально слабые места. Здесь необходимо смотреть на эту ситуацию с разных сторон, наблюдать и моделировать, что может происходить при различных вариантах развития событий, тем самым предугадывая возможные действия. Соответственно, после этого разработать превентивные меры.

Стоит отметить то, что дерево атак-контрмер в отличии от куста событий – это в первую очередь инструмент аналитика, особенно на начальной стадии формулирования и выявлений требований к абстрактной ИС. С помощью деревьев атак-контрмер легко представляются схемы последовательных действий, при этом используется классический алгоритмический аппарат. Но в тоже время, в отличии от куста событий, дерево атак-контрмер имеет сложности в наглядности, если имеет место быть нескольким действиям.

Далее, если продолжить строить подобные модели одним и тем же методом, можно в результате прийти к формальной классификации информационных угроз в зависимости от свойств модели, описывающей каждый тип – наряду с теми сугубо утилитарными и не всегда безупречными классификациями, которыми сейчас описываются угрозы. А это выводит информационную безопасность на качественно новый уровень.

Литература

1. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Тр. СПИИРАН. – 2006. –– Т. 2. – № 3. – С. 30-49.

2. Кляус Т.К., Гатчин Ю.А. Применение графического представления атак в моделировании угроз безопасности информации // Научно-технический вестник Поволжья. – 2017. – № 3. – С. 108-110.

3. Pshenichny C.A., Khrabrykh Z.V. Knowledge Base of Formation of Subaerial Eruption Unit // In S. Leroy I. Stuart (Eds.), Environmental Catastrophes and Recovery in the Holocene (Abstracts). London: Brunel University. URL: http://atlas-conferences.com/cgi-bin/abstract/caiq-22

4. Naumov A., Popov I., Bondarenko I., Krylov B., Timonin R., Ofitserov I. Dynamic Knowledge Representation as a Formalization Conveyor for Manmade Systems With Useful Impulse // Dynamic Knowledge Representaion in Scientific Domains. – 2018. – P. 270-285.

5. Kordy B., Mauw S., Radomirovic S., Schwietzer P. Foundations of attack-defense trees // Formal aspects of security and trust. – 2010. – Vol. 6561 of LNCS. – P. 1-16.

6. Кляус Т.К. Анализ состояния информационной безопасности систем электронного документооборота с помощью деревьев атак-контрмер // Сборник трудов IX Научно-практической конференции молодых ученых «Вычислительные системы и сети (Майоровские чтения)». – 2018. – С. 104-106.

7. ADTool [Электронный ресурс] // University of Luxembourg. URL: http://satoss.uni.lu/members/piotr/adtool/ (дата обращения: 23.05.2018)

8. Банькин А.А., Иванов Е.В. Метод куста событий // Сборник тезисов докладов конгресса молодых ученых (VIII Всероссийская межвузовская конференция молодых ученых, 12-15 апреля 2011 г.). – 2011. – № 1. – С. 3-4. URL: http://kmu.ifmo.ru/file/stat/12/kmu8_vep1.pdf (дата обращения: 23.05.2018)

9. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees // International journal of secure software engineering. – 2012. – Vol. 3. – № 2. – P. 1-35.

References

1. Kotenko I. V., Stepashkin M. V., Bogdanov V. S. Evaluating Security of Computer Networks based on Attack Graphs and Qualitative Security Metrics [Ocenka bezopasnosti komp'juternyh setej na osnove grafov atak i kachestvennyh metrik zashhishhennosti]. Trudy SPIIRAN [SPIIRAS Proceedings], 2006, vol. 2, no.3, pp. 30-49.

2. Klyaus T.K., Gatchin Ju.A. The use of attacks graphical representation for threat modeling [Primenenie graficheskogo predstavlenija atak v modelirovanii ugroz bezopasnosti informacii]. Nauchno-tehnicheskij vestnik povolzh'ja [Scientific and technical bulletin of the Volga region], 2017, no. 3, pp. 108-110.

3. Pshenichny C.A., Khrabrykh Z.V. Knowledge Base of Formation of Subaerial Eruption Unit. Environmental Catastrophes and Recovery in the Holocene (Abstracts), London: Brunel University. Available at: http://atlas-conferences.com/cgi-bin/abstract/caiq-22.

4. Naumov A., Popov I., Bondarenko I., Krylov B., Timonin R., Ofitserov I. Dynamic Knowledge Representation as a Formalization Conveyor for Manmade Systems With Useful Impulse. Dynamic Knowledge Representaion in Scientific Domains, 2018, pp. 270-285.

5. Kordy B., Mauw S., Radomirovic S., Schwietzer P. Foundations of attack-defense trees. Formal aspects of security and trust, 2010, vol. 6561 of LNCS, pp. 1-16.

6. Klyaus T.K. Analyzing the information security of electronic document management systems using attack-defense trees [Analiz sostojanija informacionnoj bezopasnosti sistem elektronnogo dokumentooborota s pomoshh'ju derev'ev atak-kontrmer]. Sbornik trudov IX Nauchno-prakticheskoj konferencii molodyh uchenyh "Vychislitel'nye sistemy i seti (Majorovskie chtenija)" [Proceedings of the scientific and practical conference of young scientists "Computing systems and networks (Mayorov's readings)"], 2018, pp. 104-106.

7. ADTool. University of Luxembourg. Available at: http://satoss.uni.lu/members/piotr/adtool/.

8. Ban'kin A.A., Ivanov E.V. Event bush method [Metod kusta sobytij]. Sbornik tezisov dokladov konferenzii molodyh uchenyh [Proceedings of the young scientists' conference], 2011, no. 1, pp. 3-4. Available at: http://kmu.ifmo.ru/file/stat/12/kmu8_vep1.pdf.

9. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees. International journal of secure software engineering, 2012, Vol. 3, no. 2, pp. 1-35.

КЛЯУС Татьяна Константиновна, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: t_klyaus@corp.ifmo.ru

НАУМОВ Андрей Дмитриевич, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: adnaumov@corp.ifmo.ru

ГАТЧИН Юрий Арменакович, доктор технических наук, профессор кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: gatchin@mail.ifmo.ru

БОНДАРЕНКО Игорь Борисович, кандидат технических наук, доцент кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: igorlitmo@rambler.ru

KLYAUS Tatiana, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: t_klyaus@corp.ifmo.ru

NAUMOV Andrei, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: adnaumov@corp.ifmo.ru

GATCHIN Yurii, doctor of technical sciences, professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: E-mail: gatchin@mail.ifmo.ru

BONDARENKO Igor, candidate of technical sciences, associate professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: igorlitmo@rambler.ru

УДК 004.4.056 Вестник УрФО № 2(28) / 2018, с. 43–48

Соколов А. Н., Алабугин С. К., Пятницкий И. А.

ПРИМЕНЕНИЕ МЕТОДОВ ОДНОКЛАССОВОЙ КЛАССИФИКАЦИИ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Современные тенденции в информационной безопасности характеризуются распространением комплексных целевых атак. Одним из способов борьбы со сложными сетевыми атаками, которые не всегда могут быть обнаружены классическими средствами защиты, является выявление аномалий в сетевом трафике. Для реализации такого подхода разумно использовать методы машинного обучения. В работе рассмотрены вопросы применения методов одноклассовой классификации как одной из техник машинного обучения для обнаружения вторжений, а также предложен вариант архитектуры системы обнаружения вторжения, основанной на таких методах.

Ключевые слова: *обнаружение вторжений, машинное обучение, обнаружение сетевых атак, одноклассовая классификация.*

Sokolov A. N., Alabugin S. K., Pyatnitsky I. A.

APPLYING OF ONE-CLASS CLASSIFICATION METHODS FOR INTRUSION DETECTION

The wider spread of complex target attacks is typical for the current state of information security. One way to deal with complex network attacks, which are difficult to detect by classic methods of protection, is the detection of anomalies in network traffic. It is reasonable to use machine learning methods, to implement this approach.

The paper deals with the application of one-class classification methods as one of the machine learning techniques for detecting intrusions, and proposes an architecture variant of an intrusion detection system based on such methods.

Keywords: *intrusion detection, machine learning, detection of network attacks, one-class classification.*

По данным компании Positive Technologies число компаний, столкнувшихся с целевыми атаками, за 2017 год увеличилось почти вдвое [1]. Кроме того, как отмечают эксперты, наблюдается рост сложности таких атак, в частности, злоумышленники активно применяют методы, затрудняющие анализ и расследование инцидентов.

В сложившейся ситуации классические методы, применяемые для обнаружения и защиты от вторжений [2], которые основаны на использовании сигнатур и правил, не всегда

в состоянии обнаружить атаку, не встречавшуюся ранее. Для обнаружения целевых атак предлагается использовать подход, основанный на выявлении аномалий сетевого трафика с применением техник и методов машинного обучения.

Существует два основных подхода, которые используются для обнаружения сетевых атак: обнаружение аномалий и сигнатурный подход [3]. В основе сигнатурного подхода лежит предположение, что любая сетевая атака может быть представлена уникальным шаблоном (сигнатурой атаки), а процесс обнаружения атак заключается в поиске их сигнатур. Этот подход обеспечивает малое число ложно положительных срабатываний (ошибок II рода): сигнатуры специально подбираются так, чтобы точно распознавать известные атаки. Однако в случае, если анализируется новая атака, для которой нет известной сигнатуры, её выявление проблематично. Кроме того, при реализации этого подхода, возникают такие сложности, как необходимость в постоянной актуализации базы известных атак и покрытия как можно большего числа родственных атак меньшим числом правил [3].

Обнаружение вторжений с помощью выявления аномалий предполагает построение систематически обновляющегося профиля нормальной активности характерной для сети, который содержит информацию о характерных сетевых пакетах и соединениях. Для построения профиля нормальной активности используются некоторые признаки (атрибуты) сетевого трафика [3]. При существенном расхождении наблюдаемых признаков с текущим профилем, делается вывод, что имеет место некая аномальная активность.

В основе подхода, основанного на обнаружении аномалий, лежит гипотеза, что к их появлению приводит любое вторжение. При этом аномалия может не быть атакой или вторжением. Появление аномалии также может быть связано с добавлением новых программных и аппаратных средств, неисправной работой сетевых устройств или деятельностью привилегированных пользователей сети. Поэтому описанный подход приводит к увеличению ошибок II рода. При этом если атака не приводит к появлению аномалий, она не может быть обнаружена. Кроме того, построение и систематическое обновление профиля нормальной активности, как правило, является трудоемкой и требовательной к вычислительным ресурсам задачей. Однако, применение подхода, основанного на выявлении аномалий, позволяет обнаруживать неизвестные сетевые атаки.

Таким образом, оба подхода имеют свои недостатки. Поэтому для обеспечения безопасности на практике разумно использовать их комбинацию.

Существует большое количество различных методов обнаружения сетевых атак, основанных на выявлении аномалий сетевого трафика [4]. Основной предпосылкой для применения методов машинного обучения в рамках этой задачи является отсутствие необходимости вручную создавать правила, согласно которым различаются аномалии и нормальная активность.

Под методами машинного обучения понимают, в частности, алгоритмы классификации (обучение с учителем) и кластеризации (обучение без учителя). Большинство работ в области обнаружения вторжений с применением машинного обучения используют алгоритмы классификации. Классические алгоритмы классификации, такие как метрические и линейные классификаторы, сети Байеса, деревья принятия решения и др. разработаны таким образом, чтобы классифицировать данные на несколько классов (например, классы «нормальный трафик» и «аномалия»). При этом обучаться такие алгоритмы также должны на данных, соответствующих разным классам.

Однако классические алгоритмы классификации по сути своей не приспособлены для обнаружения новых атак. Так, алгоритмы, обученные на выборке, состоящей из объектов, представляющих собой нормальный трафик и какие-либо виды сетевых атак, может классифицировать объект, представляющий новую для него атаку, как нормальный трафик. Кроме того, так как каждой компьютерной сети соответствует свой профиль нормального трафика, а алгоритм классификации каждый раз должен обучаться под конкретную компьютерную сеть, возникает проблема: как и где получить данные, соответствующие аномалиям (сетевым атакам) в конкретной компьютерной сети? Это решается, в частности, посредством генерации синтетических примеров данных, соответствующих аномалиям [3] или обучения с переносом опыта (transfer learning) [5].

В качестве альтернативного варианта, предлагается использовать алгоритмы одно-

классовой классификации. Одноклассовые классификаторы обучаются на примерах только одного класса, который в нашем случае соответствует нормальной активности, и строят решающее правило, согласно которому принимается решение о принадлежности объекта к нормальному классу [5].

К системе обнаружения вторжений (СОВ), использующей методы выявления аномалий, предъявляется ряд требований [3]:

1. Способность с высокой точностью выявлять аномалии в сети.

2. Малое количество ложных тревог.

3. Число входных параметров алгоритма должно быть небольшим, а их влияние на работу системы – низким.

4. Способность выявлять скрытые атаки.

5. Способность выявлять неизвестные системе атаки.

Процесс применения *СОВ на основе выявления аномалий характеризуется* четырьмя этапами [3]:

1. Сбор сетевого трафика.

2. Извлечение из трафика данных, представление их в виде признакового описания.

3. Анализ полученных данных и их разделение на нормальный и аномальный классы.

4. Обучение алгоритма на размеченных данных.

С учетом выше изложенных принципов и требований, предложена архитектура СОВ, использующей методы одноклассовой классификации. Схема ресурсов СОВ представлена на рис. 1.

приниматься вторым классификатором. Второй классификатор более сложный, медленный и работает с более большим количеством информации, включая информацию о состоянии сети и типичном поведении пользователей. Использование двух классификаторов в предложенной схеме мотивируется стремлением к одновременному обеспечению быстрой работы системы и высокой точности выявления аномалий. Для достижения этих целей первый классификатор должен отвечать следующим требованиям:

1. Высокая скорость обучения и работы.

2. Малый процент ложно отрицательных срабатываний (ошибок I рода).

Выберем алгоритм классификации, соответствующий сформулированным требованиям. Большинство алгоритмов одноклассовой классификации относятся либо к метрическим алгоритмам, которые основаны на вычислении функции расстояния в пространстве объектов, либо являются одной из большого числа модификаций метода опорных векторов. В ходе работы был рассмотрен ряд алгоритмов, обучающихся на примерах преимущественно одного класса. Чтобы выяснить, какой из них лучше подходит для использования в предложенной схеме СОВ, проведены эксперименты на наборах данных KDD'99 и NSL KDD [8], а также использованы результаты работ [9, 10]. Наборы данных KDD'99 и NSL KDD применяются для тестирования алгоритмов детектирования сетевых атак и широко используются исследователями.

Рис. 1. Схема ресурсов системы обнаружения вторжений.

Отличительной особенностью предложенной системы является использование двух одноклассовых классификаторов: первый отвечает за распознавание типового нормального трафика, в случае же если он посчитает объект аномалией, решение будет

В наборе NSL KDD содержатся: обучающая выборка с информацией о 125973 сетевых соединениях и тестовая выборка с информацией о 22544 сетевых соединениях.

Параметры, характеризующие каждое соединение, делятся на 4 группы:

1. Основные параметры каждого сетевого соединения.

2. Параметры, связанные с контентом каждого сетевого соединения.

3. Параметры, связанные с временными характеристиками каждого сетевого соединения.

4. Параметры, связанные с характеристиками хоста каждого сетевого соединения.

Полученные результаты представлены в табл. 1.

Таблица 1

Результатов реализации алгоритмов одноклассовой классификации на наборах данных KDD'99 и NSL KDD

Алгоритм	Набор данных	Точность	Доля неправильно распознанных атак
K-NN	KDD'99	0,974	0,72
Kth-NN	KDD'99	0,979	0,64
LOF	KDD'99	0,596	0,56
LOF-UB	KDD'99	0,577	0,55
COF	KDD'99	0,554	0,79
LoOP	KDD'99	0,574	0,78
INFLO	KDD'99	0,552	0,73
aLOCI	KDD'99	0,655	0,67
oc-SVM	KDD'99	0,951	0,26
η-oc-SVM	KDD'99	0,794	0,34
SVDD	NSL KDD	0,963	0,23
OCSVM	NSL KDD	0,941	0,24

По данным табл. 1 можно сделать вывод, что алгоритмы, основанные на методе опорных векторов (SVDD, OCSVM, oc-SVM, η-oc-SVM) имеют более высокую точность и распознают большее число атак. Однако, как и практически все модификации метода опорных векторов, эти алгоритмы сталкиваются с необходимостью во время обучения решать задачу квадратичного программирования [6], что негативно сказывается на их производительности. Кроме того, метод опорных векторов как модель алгоритма содержит большое количество параметров, которые необходимо варьировать в процессе обучения для достижения наилучшего результата. Это также добавляет сложностей при их практическом применении.

В качестве Классификатора 1 предложенной выше схемы предлагается использовать алгоритм, основанный на вычислении расстояния Махаланобиса [6, 7]. Он отчасти опирается на идеи, используемые в методе опорных векторов: используются понятие опорного вектора и отображение объектов в признаковое пространство большей размерности. При этом он спроектирован так, что решать задачу квадратичного программирования на стадии обучения не приходится.

В экспериментах с набором данных NSL KDD реализация описанного выше алгоритма на языке Python показала точность 0,95. Доля неправильно распознанных атак составила 0,102.

Таким образом, при анализе применимости методов одноклассовой классификации для обнаружения вторжений предложена схема работы системы обнаружения вторжений и исследованы возможности применения отдельных алгоритмов для выявления аномалий сетевого трафика на примере набора данных NSL KDD. Подводя итог, можно заключить, что применение методов одноклассовой классификации является перспективным способом повышения защищенности информационной системы от нетиповых, в том чисел целевых, атак.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

[1] Итоги года и прогнозы от Positive Technologies [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/288913/, свободный (дата обращения 13.06.2018)

[2] Мазиков К.И. Анализ современных сертифицированных средств обнаружения вторжений в информационных сетях // Вестник Тамбовского университета. Серия: Естественные и технические науки. – 2014. – №2. – С. 661-662

[3] Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network Traffic Anomaly Detection: Concepts, Techniques, and Tools, Springer, 2017, 262 p.

[4] Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак, Тр. СПИИРАН, 45 (2016), С. 207–244

[5] Zhao, J., Shetty, S. and Pan, J.W., 2017, October. Feature-based transfer learning for network security. In Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE (pp. 17-22). IEEE.

[6] Nader P., Honeine P., Beauseroy P. Mahalanobis-based one-class classification //Machine Learning for Signal Processing (MLSP), 2014 IEEE International Workshop on. – IEEE, 2014. – С. 1-6.

[7] Nader P., Honeine P., Beauseroy P. Online one-class classification for intrusion detection based on the mahalanobis distance //Proc. 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. – 2015. – С. 1-6.

[8] Tavallaee M. et al. A detailed analysis of the KDD CUP 99 data set //Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. – IEEE, 2009. – С. 1-6.

[9] Goldstein M., Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data //PloS one. – 2016. – Т. 11. – №. 4. – С. 152-173.

[10] Kumar S., Nandi S., Biswas S. Research and application of one-class small hypersphere Support Vector Machine for Network anomaly detection //Communication Systems and Networks (COMSNETS), 2011 Third International Conference on. – IEEE, 2011. – С. 1-4.c

Refereces

[1] Itogi goda i prognozy ot Positive Technologies. Available at: https://www.ptsecurity.com/ru-ru/about/news/288913/ (acessed 13.06.2018).

[2] Mazikov K.I. Analiz sovremennykh sertifitsirovannykh sredstv obnaruzheniya vtorzheniy v informatsionnykh setyakh // Vestnik Tambovskogo universiteta. Seriya: Estestvennyye i tekhnicheskiye nauki. – 2014. – №2. – P. 661-662.

[3] Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network Traffic Anomaly Detection: Concepts, Techniques, and Tools, Springer, 2017, 262 p.

[4] Branitskiy A. A., Kotenko I. V. Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak, Tr. SPIIRAN, 45 (2016). P. 207–244.

[5] Zhao, J., Shetty, S. and Pan, J.W., 2017, October. Feature-based transfer learning for network security. In Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE (pp. 17-22). IEEE.

[6] Nader P., Honeine P., Beauseroy P. Mahalanobis-based one-class classification //Machine Learning for Signal Processing (MLSP), 2014 IEEE International Workshop on. – IEEE, 2014. – P. 1-6.

[7] Nader P., Honeine P., Beauseroy P. Online one-class classification for intrusion detection based on the mahalanobis distance //Proc. 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning. – 2015. – P. 1-6.

[8] Tavallaee M. et al. A detailed analysis of the KDD CUP 99 data set //Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. – IEEE, 2009. – P. 1-6.

[9] Goldstein M., Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data //PloS one. – 2016. – T. 11. – №. 4. – P. 152-173.

[10] Kumar S., Nandi S., Biswas S. Research and application of one-class small hypersphere Support Vector Machine for Network anomaly detection //Communication Systems and Networks (COMSNETS), 2011 Third International Conference on. – IEEE, 2011. – P. 1-4.

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д 76. E-mail: sokolovan@susu.ru

АЛАБУГИН Сергей Константинович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д 76. E-mail: sergei_alabugin@mail.ru

ПЯТНИЦКИЙ Илья Альбертович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д 76. E-mail: Ankidoom@gmail.com

SOKOLOV Alexander, Candidate of Engineering Science, Docent, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

ALABUGIN Sergei, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sergei_alabugin@mail.ru

PYATNITSKY Ilya, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: Ankidoom@gmail.com

УДК 004.056.5 + 340.7 Вестник УрФО № 2(28) / 2018, с. 49–52

Соколов С. С., Бориев З. В.

ПРОТИВОРЕЧИЯ В ПРАВОВОМ РЕГУЛИРОВАНИИ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ

В статье проводится анализ вопросов безопасности персональных данных. Автором приведены исторические примеры обеспечения безопасности персональных данных в различных странах мира, а также классификация типов персональных данных.

Отдельным вопросом рассматривается правовое регулирование защиты персональных биометрических данных, в первую очередь вопрос соответствия федерального законодательства РФ международным договорам и конвенциям.

Исходя из результатов анализа, автор дает рекомендации по формированию единого правового пространства внутренней безопасности международного сообщества.

Ключевые слова: *персональные данные, биометрические параметры, биометрические персональные данные, правовые нормативные документы, защита биометрических данных.*

Sokolov S. S., Boriev Z. V.

DISAGREEMENTS IN THE LAW REGULATION OF THE PROTECTION OF BIOMETRIC DATA

The article analyzes the security of personal data. The author presents historical examples of ensuring the security of personal data in various countries of the world, as well as the classification of types of personal data. A separate issue is the legal regulation of the protection of personal biometric data, primarily the issue of compliance with federal laws of the Russian Federation to international treaties and conventions. Based on the results of the analysis, the author gives recommendations on the formation of a single legal space for internal security of the international community.

Keywords: *personal data, biometric parameters, biometric personal data, law regulations, protection of biometric data.*

С каждым годом технологии с использованием биометрических данных всё больше входят в нашу повседневную жизнь. Это обусловлено постоянно растущей угрозой физической и кибернетической безопасности. Биометрические системы применяются для аутентификации субъекта по таким статическим и динамическим параметрам как отпечаток пальца, геометрия лица, сетчатка глаза, почерк, голос и т.п. Перечисленные параметры являются неотъемлемой частью каждого человека, и при их использовании в системах аутентификации, они автоматически становятся биометрическими персональными данными.

Первым нормативным документом, регулирующим защиту биометрических персональных данных, является Конвенция №108 «О защите физических лиц при автоматизированной обработке персональных данных» в 1981 г., принятая в Страсбурге Советом Европы. Цель настоящей Конвенции состоит в обеспечении на территории каждой страны Европейского Союза для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных. [1]

Немного позднее большинство государств, входивших в Европейский Союз, приняли директиву 95/46/ЕС от 24.10.1995 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». Основным предметом этого документа также было положение о защите государствами-членами ЕС основных прав и свобод физических лиц, и, в частности, их право на неприкосновенность частной жизни при обработке персональных данных. Вторым основным пунктом директивы была свобода обращения персональных данных между Государствами-членами ЕС по соображениям, связанным с защитой, предоставленной согласно предыдущему пункту.[2]

Регулярное акцентирование внимания на вопросе персональных данных, в виду появления необходимости их частого использования, привело к необходимости разделения на две категории в зависимости от степени чувствительности - обычные и специальные. В дальнейшем такое деление было принято многими странами мира и стало использоваться в национальных нормативно-правовых актах.

Российская Федерация была одной из первых стран, которая внесла в законодательство обособленное понятие биометрических персональных данных. Согласно Федеральному закону от 27.07.2006 г. 152-ФЗ «О персональных данных» персональные данные делятся на следующие категории: обычные, специальные и биометрические. [3] Целесообразность этой процедуры обусловлена спецификой биометрических данных. Если данные страховки, места жительства или паспорта могут быть со временем изменены, то отпечатки пальцев или форма ушной раковины субъекта аутентификации остаются неизменными. В странах Европейского союза по этому вопросу существует два мнения: кто-то считает, что уровень защиты всех персональных данных должен быть на одном уровне, другие же настаивают на повышении уровня защиты прав граждан в сфере обработки биометрических данных. Следствием разных представлений о необходимой степени защиты биометрических параметров стали разногласия в правовом регулировании защиты таких персональных данных.

Разногласия в правовом поле регулирования защиты биометрических данных возникают на фоне формирования общего пространства внутренней безопасности мирового сообщества. Разные государства разрабатывали различные способы обеспечения безопасности граждан с помощью современных технических решений и подходов, одним из которых стало повышение требований к средствам удостоверения личности.

В первую очередь развитие направления аутентификации личности коснулось областей, где удостоверение личности является регулярной процедурой. К таким сферам можно отнести транспортную, таможенную и миграционную службы. Огромный многолетний опыт работы этих систем показал, что информация, содержащаяся в носителях, удостоверяющих личность, часто подвергается подлогу или фальсификации. Современным решением этого вопроса стали документы, содержащие биометрическую информацию. Одним из таких примеров является биометрический паспорт.

С 2002 года США и некоторые страны Европы признают биометрию лица основной технологией идентификации для паспортов, что стало началом массового применения биометрических технологий. Российская Федерация перешла на массовую выдачу биоме-

трических заграничных паспортов с 2006 года. Не смотря на общую тенденцию улучшения процессов биометрической аутентификации, вопрос защиты передаваемых параметров личности оставался на втором плане. В качестве примера продолжим рассмотрения данного вопроса на биометрическом паспорте.

Главным отличием такого паспорта от паспорта старого образца является бесконтактный чип в пластиковой оболочке, представляющий собой микроэлектронный процессор. Пару лет назад, имея смартфон со считывателем чипов с технологией беспроводной передачи данных малого радиуса действия, за пару минут можно было получить ФИО, фотографию и прочую информацию, содержащуюся в паспорте и при том абсолютно бесплатно.

В статье 9 Федерального закона «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» говорится, что биометрические данные рук остаются только на электронном носителе, и при получении паспорта удаляются из информационных систем организации, выдавшей документ. [4] К сожалению, такие условия работы с биометрическими параметрами ставят под угрозу обеспечение информационной безопасности персональных данных граждан. [5] Возникает явная угроза хищения или подлога персональных данных личности, включая биометрические параметры, которые практически не изменяются с течением времени.

Анализируя опыт западных специалистов, выяснилось, что для исключения подобных ситуаций, международная организация гражданской авиации ИКАО в своей Конвенции о Международной гражданской авиации часть 1, том 2, пункт 12.2 «О машиносчитываемых проездных документах» [6] указывает, что если государство выдачи решает предоставлять данные отпечатков пальцев в своих электронных паспортах, хранение изображения отпечатка пальца является обязательным для обеспечения глобальной интероперабельности между классами. С одной стороны мы имеем пример решения проблемы защиты исходной информации от подлога. Но в этот же момент возникает очевидная правовая коллизия. Благодаря статье 15 Конституции РФ, применяются нормы, принятые ИКАО, т.к. международным договором Российской Федерации установлены иные правила, отличные от закона РФ. [7]

В данной статье приведена наглядная иллюстрация противоречия между нормативно-правовыми актами, регулирующими одни и те же вопросы защиты биометрических данных. Коллизии возникают на фоне формирования общего пространства внутренней безопасности мирового сообщества. Необходимо приведение к общей (международной) классификации типов персональных данных, стандартов их обработки, а также более детальной проработки вопроса правового регулирования защиты биометрических данных. Организация такой однородной среды является необходимым условием для создания единого стандарта правового регулирования использования биометрических характеристик, что очень важно на фоне интенсивно растущих интеграционных процессов.

Литература

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных г. Страсбурге 28.01.1981. [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

2. Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [рус., англ.] (Принята в г. Люксембурге 24.10.1995) (с изм. и доп. от 29.09.2003) из информационного банка «Международное право». [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

3. О персональных данных: Федеральный закон № 152-ФЗ от 27.07.2006 (ред. от 29.07.2017). [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

4. О порядке выезда из Российской Федерации и въезда в Российскую Федерацию: Федеральный закон № 114-ФЗ от 15.08.1996 (ред. от 31.12.2014). [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

5. Проблемы обеспечения информационной безопасности персональных данных граждан при подаче электронных обращений в государственные органы / А.А. Васильева, С.А. Сутягин , Е.Н. Полякова, В.В. Москвин // Вестник УрФО № 4(22) / 2016. Т. 54, с.31-34.

6. Машиносчитываемые проездные документы Международной организации гражданской авиации. Часть 1 Машиносчитываемые паспорта. Т. 2 Спецификации на электронные паспорта со средствами биометрической идентификации. Шестое издание. 2006. [Электронный ресурс]: URL: http://www.icao.int/Security/mrtd/Downloads/Doc %209303/Doc %209303 %20Russian/Doc %209303 %20 Part %201 %20Vol %202.pdf.

7. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ). [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

References

8. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg 28.01.1981). Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=121499&fld=134&dst=1000000001,0&rnd=0.879501134325201#07045743226987466 (accessed 5 February 2018).

9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Luxembourg 24.10.1995). Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=49528#023341415210354177 (accessed 8 February 2018).

10. O personal'nyh dannyh: Federal'nyj zakon № 152-FZ ot 27.07.2006 (red. ot 29.07.2017). [The law of the Russian Federation #152 from 27.07.2006 "About personal data"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed 15 January 2018).

11. O porjadke vyezda iz Rossijskoj Federacii i v#ezda v Rossijskuju Federaciju: Federal'nyj zakon № 114-FZ ot 15.08.1996 (red. ot 31.12.2014). [The law of the Russian Federation #114 from 15.08.1996 "On the procedure for leaving the Russian Federation and entry into the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_11376/ (accessed 27 January 2018).

12. Vasil'eva A.A., Sutjagin S.A., Poljakova E.N., Moskvin V.V. The problems of information security of citizens' personal data when submitting electronic applications to the state departments [Problemy obespechenija informacionnoj bezopasnosti personal'nyh dannyh grazhdan pri podache jelektronnyh obrashhenij v gosudarstvennye organy]. Vestnik UrFO № 4(22) [Herald of the UFD], 2016, no.4(22), pp. 31-34.

13. Machine Readable Travel Documents of the International Civil Aviation Organization. Part 1 Machine Readable Passports. Vol. 2 Specifications for electronic passports with means of biometric identification. Sixth edition 2006. Available at: http://www.icao.int/Security/mrtd/Downloads/Doc %209303/Doc %209303 %20Russian/Doc %209303 %20Part %201 %20Vol %202.pdf (accessed 13 December 2017).

14. Konstitucija Rossijskoj Federacii (prinjata vsenarodnym golosovaniem 12.12.1993) (s uchetom popravok, vnesennyh Zakonami RF o popravkah k Konstitucii RF ot 30.12.2008 N 6-FKZ, ot 30.12.2008 N 7-FKZ, ot 05.02.2014 N 2-FKZ, ot 21.07.2014 N 11-FKZ). [Constitution of the Russian Federation Article 15] Available at: http://www.consultant.ru/document/cons_doc_LAW_28399/54dd4e1f61e0b8fa47bff695f0c08b192a95f7a3/ (accessed 15 February 2017).

СОКОЛОВ Сергей Сергеевич, заведующий кафедрой «Комплексное обеспечение информационной безопасности», Государственный университет Морского и речного флота имени адмирала С.О. Макарова. 198035, г. Санкт-Петербург, ул. Двинская, д.5/7. E-mail: sokolovss@gumrf.ru

БОРИЕВ Замир Валерьевич, аспирант, Государственный университет Морского и речного флота имени адмирала С.О. Макарова, 198035, г. Санкт-Петербург, ул. Двинская, д.5/7. E-mail: za_mir_b@mail.ru

SOKOLOV Sergey, chef of department "Complex providing information security", Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya str, Saint-Petersburg, 198035. E-mail: sokolovss@gumrf.ru

BORIEV Zamir, graduate student, Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya str, Saint-Petersburg, 198035. E-mail: za_mir_b@mail.ru

УДК 004.056.57 + 002:004.056 Вестник УрФО № 2(28) / 2018, с. 53–59

Васильев В. И., Кириллова А. Д., Сагитова В. В.

ОБ ЭВОЛЮЦИИ ПОНЯТИЯ «ПРОФИЛЬ ЗАЩИТЫ» В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализируется понятие профиля защиты, выступающее сегодня в качестве одного из ключевых понятий при построении и оценке эффективности систем защиты информации. Отмечается основополагающая роль стандарта ГОСТ Р ИСО/МЭК 15408 в формировании и конкретном наполнении данного понятия применительно к различным классам ИТ-продуктов и систем. Обсуждаются возможные подходы к разработке и применению профилей защиты с учетом требований базовых руководящих документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России. Рассматриваются возможности расширения данного понятия на задачи обеспечения комплексной безопасности предприятий (организаций).

Ключевые слова: *информационная безопасность, защита информации, профиль защиты, системы обеспечения комплексной безопасности.*

Vasilyev V. I., Kirillova A. D. , Sagitova V. V.

ON EVOLUTION OF «PROTECTION PROFILE» NOTION IN THE SPHERE OF INFORMATION SECURITY

The notion of protection profile being now one of the key notions in developing and evaluating the information security systems is analyzed. The fundamental role of the standard GOST R ISO/IEC 15408 in forming and filling this notion applied to different classes of IT-products and systems is noted. Possible approaches to development and application of protection profiles with account of basic ruling documents by Federal Service on Technical and Expert Control (FSTEC) of Russia are discussed. The opportunities of extending this notion to the problems of providing the complex security for enterprises (organizations) are considered.

Keywords: *information security, information protection, protection profile, complex security provision systems.*

Проблемы информационной безопасности (ИБ) сегодня непосредственно касаются всех сфер нашей жизни, так или иначе связанных с применением информационных технологий (ИТ). Как свидетельствует статистика [1], рост числа угроз и уязвимостей при этом сопровождается увеличением суммарного ущерба от реализации этих угроз, объектами которых являются промышленные предприятия, государственные и коммерческие организации, медицинские и образовательные учреждения и т.п. Очевидно, что для эффективного противодействия этой тенденции необходимо комплексное применение на каждом объекте системы организационно-технических мер и мероприятий, опирающееся на научно-обоснованную нормативно-законодательную базу в области защиты информации (ЗИ) и имеющее своей конечной целью снижение уровня ожидаемых информационных рисков. Важное место при разработке комплекса таких мер и мероприятий имеют обоснованное задание требований к безопасности ИТ-продуктов и систем, оценка безопасности и возможность проведения сравнительного анализа уровня безопасности ИТ-продуктов и систем с использованием такого ключевого понятия ИБ, как профиль защиты.

История происхождения данного понятия связана прежде всего с международным стандартом ISO/IEC 15408-3-1999 («Общие критерии») и его российским аналогом (последняя версия ГОСТ Р ИСО/МЭК 15408-3-2008 [2]), где в качестве 2-х видов базовых нормативных документов, определяющих требования к безопасности ИТ-продуктов и систем, выделены **профиль защиты** (Protection Profile) и **задание по безопасности** (Security Target). В соответствии с [2], профиль защиты – это типовой набор требований безопасности, которым должны удовлетворять программно-аппаратные средства и/или системы определенного класса (обобщенно – объект оценки). Задание по безопасности – это совокупность требований к конкретной разработке, выполнение которых позволит решить поставленные задачи по обеспечению безопасности.

Профиль защиты (ПЗ) не регламентирует, каким образом должны выполняться заложенные в нем требования, тем самым предоставляя возможность разработчику системы защиты информации (СЗИ) самостоятельно выбирать средства защиты. Согласно [3], требуемое содержание ПЗ должно включать в себя следующие разделы (Таблица 1).

Таблица 1

Профиль защиты

Раздел ПЗ	Содержание раздела
Введение	Идентификация ПЗ. Аннотация
Описание объекта оценки (ОО)	Границы среды безопасности. Угрозы активам, требующим защиты (включая описание этих активов). Политика безопасности организации.
Цели безопасности	Цели безопасности ОО. Цели безопасности среды.
Требования безопасности	Функциональные требования. Требования доверия к безопасности. Требования безопасности ИТ-среды ОО.
Обоснование ПЗ	Убедительные аргументы в пользу того, что рекомендуемые требования безопасности ИТ удовлетворяют намеченным целям безопасности с учетом всех аспектов среды безопасности.

На сегодняшний день ФСТЭК России разработала и утвердила около 100 методических документов, содержащих ПЗ для различных ИТ-продуктов и систем [4], в том числе:

– ПЗ систем обнаружения вторжений;

– ПЗ межсетевых экранов;

– ПЗ средств антивирусной защиты;

– ПЗ операционных систем;

– ПЗ средств контроля отчуждения (переноса) информации со съемных машинных носителей информации;

– ПЗ средств доверенной загрузки уровня базовой системы ввода-вывода; и др.

Большая часть этих ПЗ согласуется с международной трактовкой понятия ПЗ, жестко привязанной к исходному стандарту ISO/IEC 15408 и его аналогов-национальных стандартов. В частности, предполагается, что входящие в ПЗ требования безопасности (функциональные требования, требования доверия и т.п.) должны заимствоваться только из приведенного в этих стандартах перечня типовых требований. В то же время, в последние годы получает все большее распространение точ-

ка зрения, что при таком подходе невозможны унификация, регламентирование и параметризация множества конкретных функций и характеристик сложных объектов архитектуры и структуры современных информационных систем (ИС) [5]. Отсюда понятен интерес к внедрению нового прагматического подхода к разработке и применению ПЗ, основанного на использовании совокупности адаптированных и параметризованных баз международных и национальных стандартов и открытых спецификаций, отвечающих стандартам де-факто и нормативных документов ведущих фирм (компаний).

Одним их преимуществ ПЗ является возможность их использования для проведения аудита ИБ ИС. В качестве примера подобного применения ПЗ можно привести предложенную в [6] методику оценки эффективности СЗИ ИСПДн с учетом ПЗ, построенного на базе стандарта ГОСТ Р ИСО/МЭК ТО 19791 [7]. Данный стандарт включает в себя определение и модель автоматизированной (информационной) системы, описание расширенной концепции оценки безопасности системы, методологию и процесс выполнения оценки безопасности системы, а также дополнительные критерии оценки безопасности. Требования стандарта базируются на 3-хэтапном подходе к обеспечению необходимого уровня безопасности системы:

– оценка рисков безопасности;

– уменьшение рисков посредством выбора контрмер;

– аттестация для подтверждения приемлемого уровня остаточных рисков.

В качестве базовых нормативных документов при разработке ПЗ ИС могут быть использованы руководящие документы ФСТЭК России, устанавливающие перечень требований по обеспечению безопасности различных классов ИС, таких как государственные информационные системы (ГИС) [8], информационные системы персональных данных (ИСПДн) [9], автоматизированные системы управления производственными и технологическими процессами (АСУ ТП) [10], значимые объекты критической информационной инфраструктуры Российской Федерации [11]. В каждом из этих документов, в основу которых положены ГОСТ Р ИСО/МЭК 15408-2008 и ГОСТ Р ИСО/МЭК 27001-2006, определены группы типовых требований к ЗИ, которые затем конкретизируются (уточняются) для каждой из этих групп. Оценивая степень выполнения (или невыполнения) указанных требований для конкретной ИС с помощью оценочных показателей (критериев), значения которых выставляются экспертом или группой экспертов, можно получить некоторое интегральное представление о фактическом («достигнутом») ПЗ и его соответствие «эталонному» ПЗ ИС [12, 13].

Рассмотрим ситуацию, связанную с построением ПЗ, на примере АСУ ТП [14]. Приказ ФСТЭК № 31 содержит 21 группу типовых требований (мер ЗИ в АСУ ТП), каждая из которых включает в себя от 3 до 31 конкретных требований (мер защиты), в зависимости от требуемого класса защищенности системы. Обозначим через M_{ij} частный показатель степени выполнения *j*-го требования (j=1,2,…,n_i) в *i*-й группе требований (i=1,2,…,21). Будем полагать, что M_{ij}=0, если соответствующее требование не выполняется; M_{ij}=0,5, если данное требование выполняется частично (не в полной мере) и M_{ij}=1, если это требование реализовано в полном объеме. Тогда для каждой (*i*-ой) группы требований можно вычислить групповой показатель степени выполнения заданного набора требований EV_i, выраженный в %, и абсолютный показатель NE_i числа нереализованных или частично реализованных требований к ЗИ, относящихся к i-й группе:

$$EV_i = \left(\frac{1}{n_i}\sum_{j=1}^{n_i} M_{ij}\right)\cdot 100\%;\ NE_i = n_i - \sum_{j=1}^{n_i} unit(M_{ij}),\quad (1)$$

где функция *unit*(M_{ij}) равна 1, если M_{ij}=1, и 0, если M_{ij}=0 или 0,5; n_i – число требований к ЗИ в i-й группе требований. Так, если некоторая группа требований (например, 1-ая – «Идентификация и аутентификация субъектов доступа и объектов доступа») включает в себя 8 требований (базовых мер защиты), из которых в конкретной системе полностью реализованы 6 требований, частично – 1 и не выполнено 1 требование, то имеем: n_1=8; EV_1=81,3%; NE_1=2.

На рисунке 1 приведен пример линейчатой диаграммы ПЗ, показывающей значения всех 21 групповых показателей EVi и NEi для некоторой АСУ ТП.

Анализ полученной диаграммы ПЗ позволяет оценить общий уровень защищенности АСУ ТП, выявить слабые места в системе ЗИ, наметить конкретные меры для реализации требований ФСТЭК по обеспечению безопасности АСУ ТП в полном объеме.

Дальнейшее развитие концепции ПЗ свя-

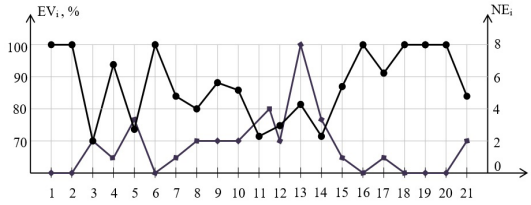

Рис.1 Диаграмма групповых показателей степени выполнения требований ПЗ (EV_i; NE_i)

зано с расширением этого понятия на задачи обеспечения комплексной безопасности предприятия (организации). В [15] под профилем защиты предприятия (объекта транспортной инфраструктуры) понимается типовой состав требований по обеспечению безопасности объекта и реализующего эти требования комплекса средств и мероприятий, обеспечивающих приемлемый уровень безопасности всего множества объектов данной категории и данного вида транспорта. Работа [16] посвящена общим методологическим вопросам построения систем обеспечения безопасности (СОБ) критически важных объектов (КВО) на базе формирования и оценки профиля защиты КВО. Под профилем защиты КВО при этом понимается независимая от реализации угроз совокупность требований безопасности для каждого типа КВО, обеспечивающая достаточную степень его защищенности. Как отмечают авторы [16], в общем случае возможны следующие постановки задачи обеспечения безопасности КВО:

1) определить эффективность функционирования СОБ при заданной модели угроз и существующем профиле защиты КВО;

2) при заданной модели угроз определить профиль защиты КВО, обеспечивающей минимальную стоимость средств защиты при допустимом уровне риска нарушения его безопасности;

3) определить профиль защиты КВО, обеспечивающий максимальный уровень безопасности объекта при заданной стоимости средств защиты.

Конструктивное определение близкого по своему смыслу и содержанию понятия «профиль безопасности объекта» вводится в [17]. По мнению автора, профиль безопасности должен включать в себя следующие разделы:

1) политика безопасности объекта – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности;

2) уровень безопасности объекта – совокупность нормативно-правовых, программно-технических и физических средств/систем защиты объекта, обеспечивающих противодействие угрозам несанкционированного доступа;

3) система аудита безопасности – совокупность методов и средств, позволяющих дать оценку проектируемой (анализируемой) системы с использованием определенного перечня оценочных критериев.

В развитие идей, изложенных в [16, 17], следует отметить, что комплексная СОБ объекта – это сложная многокомпонентная система, в силу разнородности решаемых ей задач и выполняемых ею функций состоящая из ряда относительно самостоятельных подсистем безопасности, интегрированных на основе общей информационной среды с единой базой данных. В качестве таковых подсистем обычно выступают подсистемы, отвечающие за:

– информационную безопасность;

– функциональную надежность выполнения бизнес-процессов (безопасность АСУ ТП);

– физическую защиту объекта;

– уровень квалификации и технологической дисциплины персонала;

– управление в чрезвычайных (нештатных) ситуациях.

Очевидно, что разработка системы оценочных критериев (метрик безопасности), позволяющих в полной мере оценить эффективность функционирования указанных подсистем в составе СОБ для достижения главной поставленной цели – обеспечение безопасности объекта в условиях воздействия внешних и внутренних угроз – пока еще далека от своего разрешения.

В наиболее общей постановке проблема формирования профилей интегрированных систем обеспечения комплексной безопасности (ИСОКБ) на примере предприятий наукоемкого машиностроения рассмотрена в монографии [18]. В соответствии с предложенной в этой работе концепцией, структурно ИСОКБ предприятия может быть представлена в виде спецификации программно-технических и программно-методических комплексов, образующих сложную организационно-техническую систему. В качестве профиля ИСОКБ предприятия в данном случае рассматривается упорядоченный и ограниченный набор стандартов, спецификаций требований к компонентам этой системы и

описания основных проектных решений, используемых для обеспечения безопасности бизнес-процессов предприятия. В состав базового профиля ИСОКБ предприятия при этом входят:

– описание основных компонент ИСОКБ предприятия, включая определение объектов и субъектов безопасности, процессы мониторинга и идентификации инцидентов – угроз безопасности;

– общесистемные требования к формированию информационной среды и распределенных служб обеспечения безопасности;

– требования к процессам обработки и представления данных для принятия решений на разных уровнях управления.

Достоинствами предложенного в [18] подхода является увязка целей, задач и архитектуры проектируемой ИСОКБ со спецификой бизнес-процессов предприятия, рассмотрение с единых системных позиций всех этапов жизненного цикла ИСОКБ, возможность автоматизированного анализа и проектирования профиля ИСОКБ современного предприятия, внедрение которой позволит обеспечить его безопасное функционирование и устойчивое развитие.

Подводя итоги вышесказанному, можно сделать следующие выводы. Понятие ПЗ является конструктивным и полезным в современных условиях развития ИТ, т.к. его использование дает в руки различных категорий лиц (разработчики, пользователи, аудиторы) нормативный документ, содержащий базовые требования к тому или иному классу ИТ-продуктов и систем. Сфера разработки и применения ПЗ постоянно расширяется, охватывая не только узкоспециализированные ИТ-продукты (системы обнаружения вторжений, межсетевые экраны, средства антивирусной защиты и др.), но и ИС различного назначения. Внедрение в повседневную практику руководящих документов ФСТЭК России способствует этой тенденции, инициируя разработку ПЗ для таких классов ИС, как ИСПДн, ГИС, АСУ ТП, КВО. Очередным шагом в развитии ПЗ явится построение ПЗ объектов (предприятий, организаций), приводящее в конечном итоге к созданию и внедрению интегрированных систем обеспечения комплексной безопасности этих объектов.

Статья выполнена при поддержке гранта РФФИ № 17-48-020095 «Разработка концептуальных основ и методологии математического моделирования систем обеспечения комплексной безопасности промышленных объектов».

Литература

1. Зинина О. Анализ угроз информационной безопасности 2016-2017. URL:https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_ information_security_threats_2016_2017 (дата обращения: 18.05.2018).

2. ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 3. Требования доверия к безопасности. – М.: Стандартинформ, 2009.

3. ГОСТ Р ИСО/МЭК ТО 15446-2008. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. – М.: Стандартинформ, 2010.

4. Техническая защита. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации / Методический документы. Утв. ФСТЭК России 11 мая 2017 г. URL: https://fstec.ru/technicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (дата обращения: 18.05.2018).

5. Липаев В., Филинов Е. Формирование и применение профилей открытых информационных систем // Открытые системы. СУБД, № 5, 1997. URL: https://www.osp.ru/os/1997/05/179274 (дата обращения: 18.05.2018).

6. Селифанов В.В., Звягинцева П.А., Голдобина А.С., Исаева Ю.А. Оценка эффективности системы защиты информации ИСПДн с учетом профиля защиты // Интерэкспо Гео-Сибирь, т.8, 2017. – С. 220-225.

7. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – М.: Стандартинформ, 2010.

8. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах / Утв. Приказом ФСТЭК России № 17 от 11.02.2013 г.

9. Состав и содержание организационных и технических мер по обеспечению безопасности пер-

сональных данных при их обработке в информационных системах персональных данных / Утв. Приказом ФСТЭК России № 21 от 18.02.2013 г.

10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды / Утв. Приказом ФСТЭК России № 31 от 14.03.2014 г.

11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Утв. Приказом ФСТЭК России № 239 от 25.12.2017 г.

12. Замула А.А., Северинов А.В., Корниенко М.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України, № 2 (15), 2014. – С. 133-138.

13. Датская Л.В., Кожевникова И.С., Ананьин Е.В., Оладько В.С. Автоматизация проведения аудита информационной безопасности на основе профиля защиты // Национальная ассоциация ученых (НАУ), № VI (11), 2015. Технические науки. – С. 18-22.

14. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами // Инфокоммуникационные технологии, – 2017. – т.5. - №4. – С. 319-326.

15. Стиславский А.Б. Построение профилей защиты категорируемых объектов транспортной инфраструктуры // Информационные технологии и вычислительные системы. – 2009. – №4. – С. 77-83.

16. Нечаев Д.Ю., Черешкин Д.С. Методологические аспекты интеграции систем обеспечения безопасности критически важных объектов // Изв. Российского экономического ун-та им. Г.В. Плеханова: Электронный научный журнал, № 2 (20), 2015. URL: https://www.rea.ru/ru/org/managements/izdcentr/Pages/2(20),2015.aspx (дата обращения: 18.05.2018).

17. Маликов В.В. Профили безопасности объектов различных форм собственности // Доклады БГУИР. – 2009. – № 2 (40). – С. 99-104.

18. Прохоров С.А., Федосеев А.А., Денисов В.Ф., Иващенко А.В. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения. – Самара: Самарский научный центр РАН, 2009. – 199 с.

References

1. Zinina O. Analysis of information security threats. Available at: URL:https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_ information_security_threats_2016_2017 (accessed 18 May 2018).

2. GOST R ISO/IEC 15408-3-2008 Information technology. Security techniques Evaluation criteria for IT security. Part 3. Security assurance requirements. Moscow, Standartinform, 2009.

3. GOST R ISO/IEC TO 15446-2008 Information technology (IT). Security techniques. Guide on development of protection profiles, Moscow, Standartinform, 2010.

4. Technical protection. Documents on certification of information protection tools and evaluation of informatization objects by information security requirements / Methodical documents. Appr. by FSTEC of Russia 11 May, 2017. Available at: https://fstec.ru/technicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (accessed 18 May 2018).

5. Lipaev V., Filinov E. Formation and application of open information systems profiles. Available at: https://www.osp.ru/os/1997/05/179274 (accessed 18 May 2018).

6. Selifanov V.V., Zvyagintseva P.A., Goldobina A.S., Isaeva Yu.A. Evaluation of PDIS information protection system efficiency with account of protection profile. Interexpo Geo-Sibir, v.8, 2017. P. 220-225.

7. GOST R ISO/IEC TO 19791-2008 Information technology. Security techniques. Evaluation of automated systems security. Moscow, Standartinform, 2010.

8. Requirements on protection of information not being the state mystery, containing in state information systems. Appr. by the Order of FSTEC of Russia №17 of 11.02.2013.

9. Composition and content of organizational and technical measures by providing security of private data under their processing in information systems of private data. Appr. by the Order of FSTEC of Russia № 21 of 18.02.2013.

10. Requirements on providing information protection in automated control systems of production and technological processes at critically important objects, potentially dangerous objects, and also objects representing high danger to human life and health and to natural environment / Appr. by the Order of FSTEC of Russia № 31 of 14.03.2017.

11. Requirements on providing security of significant objects of critical information infrastructure of Russian Federation / Appr. by the Order of FSTEC of Russia № 239 of 25.12.2017.

12. Zamula A.A., Severinov A.V., Kornienko M.A. Analysis of evaluation models of information security risks for constructing information security systems / Nauka i tekhnika Povitryanykh Sil Zbroinykh Sil Ukrainy, № 2 (15), 2014. P. 133-138.

13. Datskaya L.V., Kozhevnikova I.S., Ananyin E.V., Oladko V.S. Automatization of conducting information security audit on the basis of protection profile / National scientists association (NSA), № VI (11), 2015. Technical Sciences. P. 18-22.

14. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kirillova A.D. Complex evaluation of carrying out requirements to providing information protection in automated control systems of production and technological processes / Infocommunicational technologies, v.5., №4, 2017. P. 319-326.

15. Stislavsky A.B. Construction of protection profiles for categorized objects of transport infrastructure / Information technologies and computer systems, №4, 2009. P. 77-83.

16. Nechaev D.Yu., Chereshkin D.S. Methodological aspects of integrating security provision systems for critically important object / Proceedings of Russian Economical University by mane G.V. Plekhanov: Electronic scientific journal, № 2 (20). Available at: https://www.rea.ru/ru/org/managements/izdcentr/Pages/ 2(20),2015.aspx (accessed 18 May 2018).

17. Malikov V.V. Security profiles for different property forms objects / BGUIR Transactions, 2009, № 2 (40), P. 99-104.

18. Prokhorov S.A., Fedoseev A.A., Denisov V.F., Ivashenko A.V. Methods and tools of designing profiles of integrated systems of complex security provision for enterprises of scientific machine-building. Samara, Samara Scientific Center of RAN, 2009. 199 p.

ВАСИЛЬЕВ Владимир Иванович, доктор технических наук, профессор кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vasilyev@ugatu.ac.ru.

КИРИЛЛОВА Анастасия Дмитриевна, магистр, программист кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kirillova.andm@gmail.com

САГИТОВА Валентина Владимировна, аспирант кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: sagitovavv@mail.ru

VASILYEV Vladimir, Dr. Sc. (Eng.), Professor of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: vasilyev@ugatu.ac.ru.

KIRILLOVA Anastasiya, M. Sc., programmer of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kirillova.andm@gmail.com

SAGITOVA Valentina, post-graduate of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: sagitovavv@mail.ru

УДК 002:004.056 + 342.7 Вестник УрФО № 2(28) / 2018, с. 60–70

Римша А. С., Югансон А. Н., Римша К. С.

ОБ ОДНОМ ПОДХОДЕ К ФОРМИРОВАНИЮ ПЕРЕЧНЯ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ ГАЗОДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ

Удаленное и географически распределенное расположение датчиков, промышленных контроллеров, приборов автоматики в АСУ ТП увеличивает риск вторжений и атак. В данной работе дана систематизация уязвимостей беспроводных сенсорных сетей АСУ ТП газодобывающего предприятия и атак, эксплуатирующих данные уязвимости. Предложена формула для вычисления коэффициента влияния отдельной уязвимости на величину потенциального ущерба. В заключении, сформулированы задачи, решение которых позволит спроектировать и построить защищенную беспроводную сенсорную сеть. Изложен общий подход к построению защищенной беспроводной сенсорной сети.

Ключевые слова: *беспроводные сенсорные сети, киберфизическая система, информационная безопасность АСУ ТП, оценка рисков.*

Rimsha A. S., Iuganson A. N., Rimsha K. S.

ON ONE APPROACH TO THE FORMATION OF A LIST OF MEASURES TO PROTECT INFORMATION IN WIRELESS SENSOR NETWORKS OF A GAS PRODUCING ENTERPRISE

Remote and geographically distributed location of sensors, industrial controllers, automation devices in the automated process control system increases the risk of intrusions and attacks. In this paper, a systematiztion of threats and vulnerabilities is made for wireless sensor networks of the automated process control system of a typical gas producing enterprise. A formula is for calculating the coefficient of influence of an individual vulnerability on the magnitude of potential damage. In conclusion, the tasks are formulated, the solution of which will allow to design and build a protected wireless sensor network. The general approach to building a secure wireless sensor network is outlined.

Keywords: *wireless sensor networks, cyber-physical system, SCADA information security, risk assessment.*

Введение

В настоящее время применение проводных систем при эксплуатации автоматизированных систем управления технологическими процессами (АСУ ТП) не всегда эффективно из-за высокой стоимости монтажных и пусконаладочных работ, а также технического обслуживания. Кроме того, в некоторых ситуациях установка проводных датчиков вообще невозможна по технологическим или организационным причинам. Достоинствами беспроводных датчиков являются минимальные ограничения по их размещению, возможность внедрения и модификации сети таких датчиков на эксплуатируемом объекте без вмешательства в процесс функционирования, надежность и отказоустойчивость всей системы в целом при нарушении отдельных соединений между узлами [1].

В свою очередь особое внимание уделяется беспроводным сенсорным сетям (БСС): самоорганизующейся сети множества датчиков и исполнительных устройств, объединенных между собой посредством радиоканала. Данная технология имеет множество преимуществ перед классическим проводным интерфейсом передачи данных: гибкая архитектура, снижение затрат при монтаже, высокие эксплуатационные параметры и другие [2].

Практическое использование беспроводных датчиков с автономным электропитанием долгое время сдерживалось низкой надежностью радиоканала по сравнению с проводным соединением, высокими стоимостью и энергопотреблением [3]. Сейчас, благодаря развитию элементной базы, миниатюризации интегральных микросхем и появлению новых технологий передачи информации, беспроводные датчики и основанные на них системы сбора данных и мониторинга стали реальностью и применяются во многих сферах деятельности человека [1].

Однако в связи с массовым внедрением киберфизических систем, и, как следствие, развитием рынка беспроводных устройств с одной стороны, и распространением промышленного шпионажа, распространением международного терроризма, увеличением количества техногенных аварий с другой стороны, обеспечение конфиденциальности ра-

диоканала, целостности передаваемой информации, доступности беспроводных устройств и каналов связи является одной из приоритетных задач при построении новых и совершенствовании существующих систем БСС.

Прежде всего, проведем обзор публикаций, охватывающих тематику "информационной безопасности беспроводных технологий". В работе [4] приведены принципы проектирования структуры сенсорной телекоммуникационной системы на базе технологии ZigBee оптимальной, по мнению авторов, для предприятий газотранспортной отрасли. Основной недостаток, с которым приходится сталкиваться при использовании беспроводных технологий - надежность таких сетей, которую можно повысить увеличением количества сенсоров. При этом авторы не рассматривают вопросы целостности, доступности и конфиденциальности информации, передаваемой от беспроводных модулей до центра управления. В работе [5] предложены методы резервирования и планирования приоритетов, алгоритмов маршрутизации и балансировки нагрузки для повышения надежности передачи технологических данных, что положительно сказывается на доступности БСС, но никак не на передаваемой в ней информации. Статья [6] содержит классификацию по типам и источникам угроз в беспроводных сетях на сигнальном и информационном уровне, однако вопросам резервирования и повышения отказоустойчивости беспроводных сетей должного внимания не было уделено.

Таким образом, задача классификации угроз уязвимостей БСС в типовом газодобывающем предприятии для топологии БСС mesh network (самоорганизующиеся сети) является актуальной.

Систематизировав уязвимости и атаки на БСС из указанных источников можно обозначить список мероприятий для защиты БСС от этих угроз.

Цель данной статьи – сформулировать перечень актуальных угроз и определить круг задач, решение которых позволит спроектировать защищенную БСС.

Описание структуры АСУ ТП газодобывающего предприятия

Типовое газодобывающее предприятие представляет собой территориально распределенную структуру, которая начинается от кустов газовых скважин и заканчивается центральным диспетчерским пунктом [7,8]. Как правило, в промышленных АСУ ТП выделяют три уровня:

– нижний уровень — уровень датчиков и исполнительных механизмов;

– средний уровень — уровень промышленных контроллеров;

– верхний уровень — система сбора данных и оперативного диспетчерского управления (англ., SCADA – Supervisory Control And Data Acquisition).

Анализ типовой архитектуры АСУ ТП позволяет выделить четыре зоны ответственности в плане реализации мероприятий безопасности беспроводных соединений:

1) транспортную зону сбора и передачи данных на основе беспроводной сенсорной сети, в которой узлы сенсорной сети объединены с датчиками, промышленными логическими контроллерами (ПЛК) и исполнительными механизмами, где выполняются производственные и технологические процессы [9];

2) зона беспроводной передача данных между серверами ввода/вывода (SCADA) и ПЛК, использующие подключение через радиомодем или устройство широкополосного доступа (УШПД);

3) интерфейсную зону диспетчерского контроля и управления, где работают операторы и диспетчеры с целью наблюдения за ходом выполнения технологического процесса [10,11];

4) зону выхода SCADA систем во внешнюю сеть для передачи данных в центральный офис (например, GSM связь).

Первая и вторая зоны ответственности являются предметом исследования. В этих зонах наиболее сложно реализовать традиционные меры обеспечения безопасности. Рассмотрим их подробнее.

Первая зона ответственности. Во-первых, производители датчиков, контроллеров и электронной компонентной базы разрабатывают собственные закрытые протоколы функционирования, которые не позволяют внедрить технологии защиты посредством IPSec, SSL и VPN и т. п. Во-вторых, довольно часто транспортная среда представляет собой пространственно-распределенные сети на большой территории. Такие сети характерны при реализации SCADA-систем городских инженерных коммуникаций [12] (сетей тепло-, водо-, электро- и газоснабжения), нефте- и газопроводов и т. п. Здесь для передачи данных и команд используются модемные соеди-

нения (GPRS,/3G) через существующие телефонные сети и сети операторов сотовой связи публичного доступа. Для функционирования сенсорных узлов им выделяются «серые» или «белые» IP-адреса в сети мобильного оператора, что фактически означает предоставление общедоступного канала для проведения внешних атак. В-третьих, при построении сети в рамках ограниченного пространства, контроллеры и исполнительные механизмы часто подключаются по последовательному интерфейсу (RS-232/RS-485) закрытой промышленной сети к MODBUS-серверу, или по беспроводной сенсорной сети к координатору. MODBUS-сервер и координатор, как правило, имеет шлюз для выхода в корпоративную сеть предприятия и далее в Интернет с поддержкой технологий удаленного доступа и управления по протоколам стека TCP/IP. Таким образом, обеспечивается доступ к данным и узлам SCADA-системы из корпоративной предприятия и диспетчерской зон и удаленный доступ из сети Интернет [13].

Вторая зона ответственности. На практике расстояние между технологическими установками, объединенными в одну систему управления, достигает нескольких километров, поэтому с точки зрения экономической эффективности (монтаж кабеля) и повышения надежности (обрыв кабеля) на удаленных объектах часто используются решения с применением беспроводного канала связи. В зависимости от расстояния между серверами ввода/вывода и ПЛК, а также наличия интерфейсов, используются подключение через радиомодем или устройство широкополосного доступа (УШПД). От радиомодема и УШПД сигнал приходит на радиомачту, от которой подключается к промышленному коммутатору. Помимо беспроводного подключения также могут использоваться волоконно-оптические линии, которые напрямую подключаются к коммутатору, но для повышения надежности приходится резервировать такие каналы связи, что увеличивает расходы. Одними из часто используемых шин передачи данных, используемых на производстве, являются Ethernet или специальная промышленная шина Profibus DP. Цифровая сеть позволяет объединить разнесенные компоненты системы в единый программно-аппаратный комплекс.

Сенсорные узлы могут включаться в общую инфраструктуру автоматически и спонтанно и размещаться на удаленных неохраняемых объектах, поэтому они могут быть захвачены и взломаны злоумышленником с целью использования их как источников атак. В сенсорных сетях немаловажное значение имеет своевременное обнаружение и изоляция таких скомпрометированных узлов, и активная защита от атак с их стороны до момента обнаружения. Критической угрозой для беспроводной сенсорной сети является внедрение через скомпрометированные узлы кодов для кражи важных данных о контролируемых процессах или для нарушения их корректной работы [13].

Постановка проблемы

Оценка уязвимости промышленной системы – это процесс выявления, анализа, классификации уязвимостей [14] с оценкой рисков безопасности и возможного ущерба при ее эксплуатации злоумышленниками или вредоносными программами [13].

При использовании беспроводной транспортной среды для передачи данных и команд достаточно просто перехватить и подменить кадры, передаваемые по сети, на кадры с вредоносным содержимым. Можно организовать генерацию и рассылку большого числа сторонних кадров в БСС, чтобы вызвать «отказ в обслуживании» (denial-of-service – DoS-атаку) промышленного оборудования или сетевого узла [15]. И, наконец, нарушить работу радиопередающих сетевых устройств можно путем генерации мощного электромагнитного излучения в частотном диапазоне БСС импульсного характера или сигнала типа «белый шум» (jamming attack) [13].

Выделим основные причины невысокой эффективности традиционных механизмов защиты передаваемых данных [16] для обеспечения безопасности SCADA-систем с беспроводными сенсорными сетями:

1) топология и динамические маршруты в сенсорной сети строятся на основе информации, полученной от координаторов, маршрутизаторов или оконечных сенсорных узлов по принципу «маршрутизация от источника» [1];

2) при работе алгоритмов маршрутизации используется механизм широковещательной рассылки маршрутных кадров и квитанций подтверждения. Широковещательная рассылка также используется при конфигурировании сети и поиске новых узлов;

3) после построения маршрута передача кадров осуществляется последовательно по цепочке между соседними узлами по одному

маршруту, который можно разрушить или изменить в любой момент времени;

4) идентификация сенсорных узлов и кадров данных осуществляется только на основе адресной информации, полученной сенсорными узлами от координатора сети, что позволяет подменить координатор и переназначить адреса;

5) аутентификация кадров данных и узлов сети в большинстве случаев просто не выполняется, что позволяет подменить сенсорные узлы и маршрутизаторы на «чужие» узлы с вредоносной «прошивкой». Широковещательная аутентификация узлов и кадров данных являются необходимым условием обеспечения защиты и устойчивости работы БСС [13].

Оценка рисков

Для примера возьмем множество всех беспроводных датчиков, используемых в технологическом процессе:

$c_{sensor} = \{c_0^{sensor}, \dots, c_5^{sensor}\}$, где $C_0 sensor$ - приемник, $C_1 sensor, \dots, C_5 sensor$ - беспроводные датчики.

В отличие от предложенной обобщённой математической модели АСУ ТП [17] для представления взаимодействия устройств друг с другом будет использоваться сетевая модель OSI, где каждому ее уровню (физическому, канальному, сетевому, транспортному, сеансовому, представления, прикладному) будет соответствовать матрица смежности, размерность которой определяется числом компонентов системы |C|, а в качестве значений будут указываться сетевые протоколы [18]. Таким образом, множество взаимодействий устройств будет представлено в следующем виде:

$$S = \{S^1, \dots, S^7\} \quad (1),$$

где , $$S^k = \begin{vmatrix} 0 & \dots & s_{1j}^k & \dots & s_{1i}^k & \dots & s_{1n}^k \\ \dots & 0 & \dots & \dots & \dots & \dots & \dots \\ s_{j1}^k & \dots & 0 & \dots & s_{ji}^k & \dots & s_{jn}^k \\ \dots & \dots & \dots & 0 & \dots & \dots & \dots \\ s_{i1}^k & \dots & s_{ij}^k & \dots & 0 & \dots & s_{in}^k \\ \dots & \dots & \dots & \dots & \dots & 0 & \dots \\ s_{n1}^k & \dots & s_{nj}^k & \dots & s_{ni}^k & \dots & 0 \end{vmatrix}$$

k – уровень модели OSI,

s_{ij} – протоколы взаимодействия.

Беспроводные сенсорные сети организуются на двух основных топологиях [1]:

1. Mesh network – самоорганизующиеся ячеистые сети (рис. 1);

2. Звезда – жестко заданная сеть (рис. 2).

Самоорганизующиеся ячеистые сети (Mesh network) образуются на основе множества соединений типа «точка–точка», находящихся в области радиопокрытия друг друга (рис. 1).

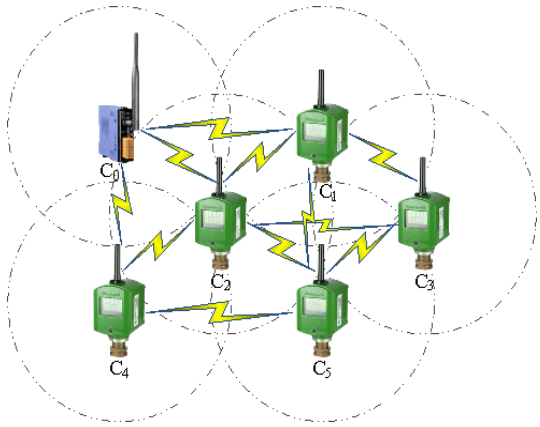

Рис. 1. Ячеистая топология самоорганизующейся сети

Такая технология позволяет беспроводным полевым приборам самостоятельно взаимодействовать друг с другом. Ключевыми преимуществами ячеистых сетей являются: автоматическое соединение между датчиками и способность любого датчика выполнять функции транзитной передачи данных для других участников сети. Сеть на основе ячеистой топологии надежна, обладает большой пропускной способностью. Высокая надежность обеспечивается наличием резервных маршрутов передачи данных: при выводе одного из датчиков из эксплуатации данные будут передаваться в обход по резервному пути, если этот датчик не являлся ключевым в этой ветке. Использование нескольких альтернативных маршрутов повышает пропускную способность сети. Снижение энергопотребления достигается снижением мощности сигналов посредством передачи данных через большее число узлов, разделенных меньшими расстояниями [17].

Топология «звезда» представляет собой централизованную систему, в которой каждое полевое устройство связывается с одной общей точкой доступа (шлюзом) напрямую. Каждый полевой прибор должен иметь прямую видимость со шлюзом, поэтому при добавлении нового устройства в сеть необходимо обеспечить прямую видимость как минимум с одной точкой доступа (рис. 2).

Далее рассмотрим влияние основных типов уязвимостей на активы БСС. Под актива-

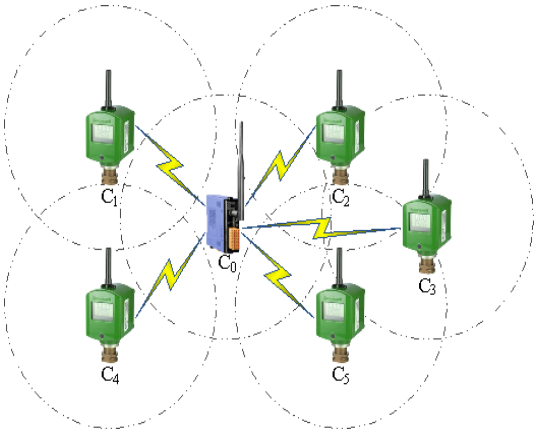

Рис. 2. Топология "звезда" для самоорганизующейся сети

ми будем рассматривать элементы беспроводной системы, под уязвимостями – условия реализации угрозы (табл. 1).

Количественное определение влияния конкретной уязвимости на определенный актив определяется экспертным путем на основе типовой модели угроз, разработанной для конкретного газодобывающего предприятия, использующего БСС в своей архитектуре АСУ ТП [19].

Влияние одной уязвимости на множество активов рассчитывается по следующей формуле:

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i \qquad (2)$$

При реализации угрозы нарушается технологический процесс, результатом которого может быть выход из строя компонентов системы [20]. Под ущербом, нанесенным в таком случае, будем понимать совокупность

Таблица 1

Матрица влияния уязвимостей на активы для беспроводных технологий

№ п/п	Уязвимости\Активы	Приемник	Передатчик	Антенны
Угрозы нарушения конфиденциальности				
1	Наличие в передаваемых данных отличительных признаков, работа на одном канале	v1,1	v1,2	v1,3
2	Использование стандартных форматов без дополнительной коррекции	v2,1	v2,2	v2,3
3	Отсутствие маскировки синхронизации и маркеров доступа	v3,1	v3,2	v3,3
4	Возможность сбора статистики передачи информации, использование при передаче открытых кодов	v4,1	v4,2	v4,3
5	Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала	v5,1	v5,2	v5,3
6	Наличие в каналах незашифрованной и расшифрованной информации	v6,1	v6,2	v6,3
7	Наличие аппаратуры на прием	v7,1	v7,2	v7,3
Угрозы нарушения целостности				
8	Наличие пересечений в сигнальных и логических областях команд и директив	v8,1	v8,2	v8,3
9	Неполная реализация протокола	v9,1	v9,2	v9,3
10	Низкая фильтрация сигналов основного канала	v10,1	v10,2	v10,3
11	Возможность определения протокола обмена	v11,1	v11,2	v11,3
12	Возможность выделения и определения идентификационных преамбул	v12,1	v12,2	v12,3
13	Наличие логического или физического адреса объекта воздействия	v13,1	v13,2	v13,3
Угрозы нарушения доступности				
14	Неполное тестирование аппаратуры	v14,1	v14,2	v14,3
15	Работа в условиях помех	v16,1	v16,2	v16,3
16	Наличие незакрепленных деталей	v17,1	v17,2	v17,3
17	Плохое экранирование приемной аппаратуры, побочные полосы	v18,1	v18,2	v18,3
18	Наличие отражающих поверхностей, низкое расположение антенн	v19,1	v19,2	v19,3

всех уязвимостей конкретной угрозы с учетом потенциального воздействия каждой.

Так как под ущербом мы подразумеваем реализацию угрозы, то оценка ущерба от конкретной угрозы будет определяться совокупностью уязвимостей, которые с ней связаны:

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right) \qquad (3)$$

Для оценки коэффициента влияния отдельной уязвимости на величину потенциального ущерба от угрозы с присутствием данной уязвимости воспользуемся следующей формулой [21]:

$$x = \frac{\sum_{i=1}^{n} P(t_i \mid c_1)}{\sum_{i=1}^{n} P(t_i)} \qquad (4)$$

где $T = \{t_i\}$ – множество не взаимосвязанных угроз информационной безопасности с присутствием конкретной уязвимости;

$P(t_i)$ – вероятность возникновения любой угрозы из множества T;

$P(t_i|c_1)$ – вероятность возникновения угрозы с присутствием конкретного уязвимости.

Систематизация уязвимостей и атак на БСС

Под атакой будет понимать попытку получить несанкционированный доступ к сервису, ресурсу либо информации. Атакой также может быть попытка скомпрометировать целостность, доступность и конфиденциальность системы.

Существует огромное множество возможных атак на системы [22]. Например, некоторые атаки могут быть направлены на перехват сообщений, их изменение и дальнейшую отправку получателю для реализации более сложных атак, таких как создание зловредных узлов с целью организации ложных шлюзов. Опираясь на исследование [23] можно выделить две группы атак: активные и пассивные.

К пассивным атакам (П) относятся атаки, направленные на прослушивание траффика, аггрегирование и несанкционированный съем информации путем внедрения в коммуникационные протоколы или с помощью мониторинга сетевых пакетов. К активным атакам (А) можно отнести атаки, связанные с внедрением помех в БСС, представление вредоносного узла в качестве легитимного, изменение сетевых потоков и их источников, создание дыр в протоколах безопасности, нарушении производительности БСС и т.д.

Выявленных уязвимостей и наиболее значимые атаки на БСС типового газодобывающего предприятия можно систематизировать следующим образом:

Заключение

В результате проведенной систематизации уязвимостей и атак на БСС типового газодобывающего предприятия, был сформирован следующий перечень задач, решение которых позволит спроектировать и построить защищенную БСС:

1) должна быть обеспечена устойчивость к активным радиопомехам;

2) должно быть настроено автоматическое обнаружение и выявление подмененных узлов сенсорной сети;

3) должны быть созданы резервные маршруты передачи данных;

4) должно быть настроено автоматическое обнаружение и предотвращение попыток реконфигурирования сети, подмены адресной информации, несанкционированной «перепрошивки» устройств;

5) должны быть использованы механизмы идентификации и аутентификации узлов и кадров;

6) должна быть обеспечена устойчивость к искажению и фильтрации кадров данных;

7) должен быть применен механизмы канального шифрования кадров данных и управления ключами.

Таблица 2

Систематизация уязвимостей и атак на БСС

Уровень	Вид атаки	Эксплуатируемые уязвимости
Физический уровень	Создание радиотехнических помех (А)	Плохое экранирование приемной аппаратуры, побочные полосы
		Работа в условиях помех
		Наличие отражающих поверхностей, низкое расположение антенн
	Несанкционированный доступ (П)	Наличие в каналах незашифрованной и расшифрованной информации
		Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала
		Наличие аппаратуры на прием
		Возможность сбора статистики передачи информации, использование при передаче открытых кодов
Канальный уровень	Коллизия (А)	Работа в условиях помех
		Плохое экранирование приемной аппаратуры, побочные полосы
	Исчерпание энергоресурсов (А)	Возможность определения протокола обмена
		Низкая фильтрация сигналов основного канала
	Анализ трафика (П)	Возможность сбора статистики передачи информации, использование при передаче открытых кодов
		Возможность определения протокола обмена
Сетевой	Выборочная переадресация (А)	Отсутствие маскировки синхронизации и маркеров доступа
		Использование стандартных форматов без дополнительной коррекции
	Ошибочная адресация (А)	Наличие в передаваемых данных отличительных признаков, работа на одном канале
		Отсутствие маскировки синхронизации и маркеров доступа
		Плохое экранирование приемной аппаратуры, побочные полосы
	Репликация узлов (А)	Неполное тестирование аппаратуры
		Наличие логического или физического адреса объекта воздействия
		Возможность выделения и определения идентификационных преамбул
	Спуфинг, имитация соединения (П)	Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала
		Наличие в передаваемых данных отличительных признаков, работа на одном канале
Транспортный	Десинхронизация, рассогласование (А)	Неполная реализация протокола
	Флудинг, лавинная рассылка (А)	Наличие пересечений в сигнальных и логических областях команд и директив
		Наличие в передаваемых данных отличительных признаков, работа на одном канале
Прикладной	Определение местонахождения узла (А)	Наличие логического или физического адреса объекта воздействия
	Отказ в обслуживании (А)	Наличие пересечений в сигнальных и логических областях команд и директив
		Низкая фильтрация сигналов основного канала
		Возможность выделения и определения идентификационных преамбул
	Переполнение (А)	Неполная реализация протокола
		Неполное тестирование аппаратуры

Литература

1. Байтимиров А.Д., Шустрова М.Л. Беспроводные технологии в промышленности // Вестник Казанского технологического университета. 2014. — № 14. — С. 473–475.

2. Бушмелев П.Е., Увайсов С.У., Плюснин И.И., Бушмелева К.И. Беспроводная сенсорная сеть обнаружения утечек газа на магистральных газопроводах // Инновационные информационные технологии. Материалы международной научно-практической конференции, 2012. — С. 377-380.

3. Богданов С.П., Басов О.О. Перспективы и проблемы применения беспроводных датчиков с автономным питанием // Доклады ТУСУРа. 2012. — № 2 (26), ч. 1. — С. 231–238.

4. Барабанова Е.А., Мальцев Д.Б., Есауленко В.Н., Руденко М.Ф. Распределенная система контроля технологических объектов нефтегазовой промышленности на базе беспроводной сенсорной сети // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. — № 2. — С. 98–104.

5. Пикалов А.И., Галимов Р.Р. Анализ методов повышения отказоустойчивости беспроводной сети распределенных систем контроля и управления технологическими объектами // Приволжский научный вестник. 2016. — № 6 (58). — С. 23–27.

6. Карцан Р.В., Карцан И.Н. Беспроводной канал передачи информации, и ее защита // Актуальные проблемы авиации и космонавтики. 2015. — Т. 1. № 11. — С. 494–496.

7. Khan W.Z. Oil and Gas monitoring using Wireless Sensor Networks: Requirements, issues and challenges // Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2016 International Conference on. — IEEE, 2016. — PP. 31-35.

8. Масагутов Р. АСУ ТП установки подготовки газа с расширенной функциональностью системы ПАЗ // Современные технологии автоматизации. 2012. — № 2. — С. 20–29.

9. Zhu C. A virtual grid-based real-time data collection algorithm for industrial wireless sensor networks // EURASIP Journal on Wireless Communications and Networking. 2018. — Vol. 2018. — № 1. — P. 134.

10. Taboun M.S., Brennan R.W. An Embedded Multi-Agent Systems Based Industrial Wireless Sensor Network // Sensors. 2017. — Vol. 17. — №. 9. — P. 2112.

11. Taboun M.S., Brennan R.W. An Embedded Agent-Based Intelligent Industrial Wireless Sensor Network // International Conference on Industrial Applications of Holonic and Multi-Agent Systems. — Springer, Cham, 2017. — PP. 227-239.

12. Синещук М.Ю. Особенности обеспечения информационной безопасности АСУ ТП потенциально опасных объектов // Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций. 2015. — № 1 (6). — С. 49–51.

13. Финогеев А.Г., Нефедова И.С., Тхай К.В. Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП // Известия ВолгГТУ. 2014. — № 6 (133). — С. 66–72.

14. Shcherbakov M.V., Brebels A., Shcherbakova N.L., Tyukov A.P., Janovsky T.A., Kamaev V.A. A Survey of Forecast Error Measures // World Applied Sciences Journal (WASJ). 2013. — Vol. 24, Spec. Issue 24: Information Technologies in Modern Industry, Education & Society. — PP. 171–176.

15. Агафонов А.В., Синадский Н.И. Структура и принцип работы комплекса тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании» // Вестник УрФО. Безопасность в информационной сфере. 2015. — № 4 (18). — С. 4–11.

16. Финогеев А.Г., Нефедова И.С., Тхай Куанг Винь. Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП // Известия ВолгГТУ. 2014. — № 6 (133). — С. 66–72.

17. Захаров А.А., Римша А.С., Харченко А.М., Зулькарнеев И.Р. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия // Вестник УрФО. Безопасность в информационной сфере. 2017. — № 3 (25). — С. 24–33.

18. Cao N. The Comparisons of Different Location-Based Routing Protocols in Wireless Sensor Networks // Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on. – IEEE, 2017. — Vol. 2. — PP. 324-327.

19. Taylor J.H. Intelligent control and asset management: An event-based control road map // Paper presented at the 2016 2nd International Conference on Event-Based Control, Communication, and Signal Processing. EBCCSP 2016 — Proceedings, doi:10.1109/EBCCSP.2016.7605269

20. Римша А.С. К вопросу об информационной безопасности автоматизированных систем управления технологическими процессами газодобывающего предприятия // Сборник тезисов докладов: Вторая Арктическая совместная науч.-практ. конф., Новый Уренгой, 16-19 мая 2018 / ООО «Газпром добыча Уренгой» и «Газпром добыча Ямбург», 2018. — С. 84-85.

21. Дерендяев Д.А., Гатчин Ю.А., Безруков В.А. Математическая модель оценки коэффициента вли-

яния отдельно взятого фактора на угрозы информационной безопасности // Кибернетика и программирование. 2016. — № 5. — С. 83–88.

22. Chhaya L. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control // Electronics. — 2017. — Vol. 6. — № 1. — P. 5.

23. Mohammadi S., Jadidoleslamy H.A comparison of link layer attacks on wireless sensor networks. // International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks. 2011. — № 3 (1), PP. 69–84.

References

1. Baitimirov A.D., Shustrova M.L. Wireless Technologies in Industry [Besprovodnye tekhnologii v promyshlennosti] // Vestnik Kazanskogo tekhnologicheskogo universiteta. 2014. — № 14. — PP. 473–475.

2. Bushmelev P., Uvaysov S., Plusnin I., Bushmeleva K. Wireless sensor network detection of leaks on the main gas pipelines [Besprovodnaya sensornaya set obnaruzheniyautechek gaza na magistralnykh gazoprovodakh] // Innovative information technologies. Materials of the International Scientific and Practical Conference, 2012. — PP. 377-380.

3. Bogdanov S.P., Basov O.O. Prospects and Problems of Using Wireless Sensors with Autonomous Power Supply [Perspektivy i problemy primeneniia besprovodnykh datchikov s avtonomnym pitaniem] // Doklady TUSURa. 2012. — № 2 (26), ch. 1. — PP. 231–238.

4. Barabanova E.A., Maltsev D.B., Esaulenko V.N., Rudenko M.F. Distributed Control System for Technological Objects of Oil and Gas Industry on the Basis of Wireless Sensor Network [Raspredelennaia sistema kontrolia tekhnologicheskikh obieektov neftegazovoi promyshlennosti na baze besprovodnoi sensornoi seti] // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitelnaia tekhnika i informatika. 2017. — № 2. — PP. 98–104.

5. Pikalov A.I., Galimov R.R. Analysis of Methods for Increasing the Fault Tolerance of a Wireless Network of Distributed Monitoring and Control Systems for Technological Objects [Analiz metodov povysheniia otkazoustoichivosti besprovodnoi seti raspredelennykh sistem kontrolia i upravleniia tekhnologicheskimi obieektami] // Privolzhskii nauchnyi vestnik. 2016. — № 6 (58). — PP. 23–27.

6. Kartsan R.V., Kartsan I.N. Wireless Channel of Information Transmission and its Protection [Besprovodnoi kanal peredachi informatsii, i ee zashchita] // Aktualnye problemy aviatsii i kosmonavtiki. 2015. — Vol. 1. № 11. — PP. 494–496.

7. Khan W.Z. Oil and Gas monitoring using Wireless Sensor Networks: Requirements, issues and challenges // Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2016 International Conference on. — IEEE, 2016. — PP. 31-35.

8. Masagutov R. APCS of the Gas Preparation Unit with Extended Functionality of the PA System [ASU TP ustanovki podgotovki gaza s rasshirennoi funktsionalnostiu sistemy PAZ] // Sovremennye tekhnologii avtomatizatsii. 2012. — № 2. — PP. 20–29.

9. Zhu C. A virtual grid-based real-time data collection algorithm for industrial wireless sensor networks // EURASIP Journal on Wireless Communications and Networking. 2018. — Vol. 2018. — № 1. — P. 134.

10. Taboun M.S., Brennan R.W. An Embedded Multi-Agent Systems Based Industrial Wireless Sensor Network // Sensors. 2017. — Vol. 17. — №. 9. — P. 2112.

11. Taboun M.S., Brennan R.W. An Embedded Agent-Based Intelligent Industrial Wireless Sensor Network // International Conference on Industrial Applications of Holonic and Multi-Agent Systems. — Springer, Cham, 2017. — PP. 227-239.

12. Sineshchuk M.I. Features of Ensuring Information Security of Automated Process Control Systems of Potentially Dangerous Objects [Osobennosti obespecheniia informatsionnoi bezopasnosti ASU TP potentsialno opasnykh obieektov] // Sovremennye tekhnologii obespecheniia grazhdanskoi oborony i likvidatsii posledstvii chrezvychainykh situatsii. 2015. — № 1 (6). — PP. 49–51.

13. Finogeev A.G., Nefedova I.S., Tkhai K.V. Security Problems of a Wireless Sensor Network in SCADA Systems of Automated Process Control Systems [Problemy bezopasnosti besprovodnoi sensornoi seti v SCADA-sistemakh ASU TP] // Izvestiia VolgGTU. 2014. — № 6 (133). — PP. 66–72.

14. Shcherbakov M.V., Brebels A., Shcherbakova N.L., Tyukov A.P., Janovsky T.A., Kamaev V.A. A Survey of Forecast Error Measures // World Applied Sciences Journal (WASJ). 2013. — Vol. 24, Spec. Issue 24: Information Technologies in Modern Industry, Education & Society. — PP. 171–176.

15. Agafonov A., Sinadsky N. Structure and operation principle of the hardware and software complex intended for testing the immunity of telecommunication equipment against denial of service network attacks [Struktura i printsip raboty kompleksa testirovaniya ustoychivosti telekommunikatsionnogo oborudovaniya k setevym atakam tipa «otkaz v obsluzhivanii»] // Vestnik UrFO. Bezopasnost v informatsionnoi sfere. 2015. — № 4 (18). — PP. 4–11.

16. Finogeev A.G., Nefedova I.S., Tkhai Kuang Vin. Security Problems of a Wireless Sensor Network in SCADA Systems of Automated Process Control Systems [Problemy bezopasnosti besprovodnoi sensornoi seti v SCADA-sistemakh ASU TP] // Izvestiia VolgGTU. 2014. — № 6 (133). — PP. 66–72.

17. Zakharov A.A., Rimsha A.S., Kharchenko A.M., Zulkarneev I.R. Analysis of Information Security of Automated Control Systems for Technical Processes of a Gas Producing Enterprise [Analiz informatsionnoi bezopasnosti avtomatizirovannykh sistem upravleniia tekhnicheskimi protsessami gazodobyvaiushchego predpriiatiia] // Vestnik UrFO. Bezopasnost v informatsionnoi sfere. 2017. — № 3 (25). — PP. 24–33.

18. Cao N. The Comparisons of Different Location-Based Routing Protocols in Wireless Sensor Networks // Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on. – IEEE, 2017. — Vol. 2. — PP. 324-327.

19. Taylor J.H. Intelligent control and asset management: An event-based control road map // Paper presented at the 2016 2nd International Conference on Event-Based Control, Communication, and Signal Processing. EBCCSP 2016 — Proceedings, doi:10.1109/EBCCSP.2016.7605269

20. Rimsha A.S. The problem of information security of automated control systems for technical processes of a gas producing enterprise [K voprosu ob informatsionnoy bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami gazodobyvayushchego predpriyatiya] // Proceedings of the Second Arctic joint scientific-practical conference, 2018. — PP. 84-85.

21. Derendiaev D.A., Gatchin I.A., Bezrukov V.A. A Mathematical Model for Estimating the Coefficient of Influence of an Individual Factor on Threats to Information Security [Matematicheskaia model otsenki koeffitsienta vliianiia otdelno vziatogo faktora na ugrozy informatsionnoi bezopasnosti] // Kibernetika i programmirovanie. 2016. — № 5. — PP. 83–88.

22. Chhaya L. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control // Electronics. — 2017. — Vol. 6. — № 1. — P. 5.

23. Mohammadi S., Jadidoleslamy H. A comparison of link layer attacks on wireless sensor networks. // International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks. 2011. — № 3 (1). — PP. 69–84.

РИМША Андрей Сергеевич, аспирант кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaAndrew@gmail.com

Югансон Андрей Николаевич, аспирант кафедры проектирования и безопасности компьютерных систем. Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 197101, г. Санкт-Петербург. Кронверкский пр., 49. E-mail: a_yougunson@corp.ifmo.ru

Римша Константин Сергеевич, студент кафедры информационной безопасности. Тюменский государственный университет. 625003, г. Тюмень. ул. Перекопская 15а. E-mail: RimshaKonstantin@ya.ru

RIMSHA Andrew, post-graduate student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaAndrew@gmail.com

IUGANSON Andrei, post-graduate student of the Department of Computer System Design and Security. ITMO University. Bld. 49, Kronverksky avenue, Saint-Petersburg, 197101. E-mail: a_yougunson@corp.ifmo.ru

RIMSHA Constantin, student of the Information Security Department. Tyumen State University. Bld. 15a, Perekopskaya Str., Tyumen, 625003. E-mail: RimshaKonstantin@ya.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые

Подпись, дата

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта или заключение от экспертной комиссии.

Библиографические ссылки

Цитируемая в статье литература приводится в виде списка в конце текста. В тексте в квадратных скобках дается ссылка на порядковый номер списка (ГОСТ Р 7.0.5.-2008). Полный текст ГОСТа размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии Авторские примечания (не являющиеся используемой литературой или ссылкой на источник) размещаются в постраничных сносках.

Ниже приводятся образцы оформления сносок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76, ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 2(28) / 2018

Дата выхода в свет 30.06.2018. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 4,20. Тираж 100 экз. Заказ 12/36.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 2(28) / 2018

Date of publication of the 30.06.2018. Format 70×108 1/16. Screen printing.
Conventional printed sheet 4,20. Circulation – 100 issues. Order 12/36. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080