ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(15) / 2015

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-44941 от 05.05.2011

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

Адрес редакции: 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**

В НОМЕРЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИОННАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРАКТИЧЕСКИЙ АСПЕКТ

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

COMPUTER SECURITY

MATHEMATICAL METHODS IN INFORMATION SECURITY

ORGANIZATIONAL AND LEGAL PROTECTION INFORMATION

THE PRACTICAL ASPECT

УДК 004.422 + 004.738.5.056.5 + 342.2/.7 : 004.056 + 378.031.4

Гузенкова Е. А.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Рассматриваются облачные сервисы, необходимые для удаленного выполнения работ по дисциплинам студентами и обеспечения информационной безопасности облачной среды виртуализации и хранения информации в облаке. В статье приведены преимущества применения облачных технологий на базе платформ VMwarevSphere с обработкой данных ограниченного доступа в виртуальной среде – vGate. Данное решение обеспечивает защиту средств управления виртуальной инфраструктурой и обладает функционалом мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Сервер авторизации vGate защищает периметр сети администрирования и разграничивает доступ серверам виртуализации и к средствам управления виртуальной инфраструктуры, а также обладает многими средствами защиты информации, при работе с ней в облачных технологиях, что позволяет реализовывать лабораторные работы на базе частного облака университета.

Ключевые слова: *облачные сервисы, виртуализация рабочих мест, частное облако, средства защиты*

Guzenkova E. A.

PROVIDING INFORMATION SECURITY CLOUD IN THE IMPLEMENTATION OF TECHNOLOGIES TO EDUCATIONAL PROCESS

Cloud services are considered necessary for the remote execution of works by students in the disciplines of information security and cloud virtualization and data storage in the cloud. The

article presents the advantages of using cloud-based platforms with VMware vSphere data processing restricted in a virtual environment - vGate. The solution protects virtual infrastructure management tools and has a functional mandate and discretionary access control to the objects that are placed inside the protected perimeter. The authorization server protects the network perimeter vGate administration and delineates the access server virtualization and virtual infrastructure management tools, and has many means of information protection, while working with her in the cloud technology, which allows to realize laboratory works on the basis of a private cloud University.

Keywords: *cloud computing, desktop virtualization, private cloud, remedies*

В современном мире все большее распространение получают облачные вычисления. За последние годы концепция облачных вычислений стала более востребована, в том числе как платформа для поддержки образовательной деятельности [1].

Сегодня под облачными вычислениями обычно понимают возможность получения необходимых вычислительных мощностей по запросу из сети.

С ростом числа часов самостоятельного изучения дисциплин становится актуальным перенос части лабораторного практикума из аудиторного фонда университета на внеклассное изучение предмета студентами. Основная проблема заключается в том, что оборудование, которым обладает студент, может обладать недостаточной мощностью, для осуществления лабораторного практикума, а также не иметь лицензий на программное обеспечение.

Для большей вовлеченности учащегося в процесс обучения можно реализовать групповую работу над заданиями с помощью удаленного доступа.

Несмотря на привлекательность создания виртуального рабочего пространства или хранения информации на основе облачных технологий, у них имеется ряд минусов, которые до сих пор являются тормозящим фактором для повсеместного применения данной инфраструктуры в России.

Один из них заключается в необходимости постоянного соединения с сетью Интернет с большой пропускной способностью, то есть скорость работы облачной площадки будет зависеть от пропускной способности канала, и если она невелика, то программное обеспечение может работать с большой задержкой по сравнению с локально установленным ПО.

Другим недостатком является то, что при использовании сторонних облачных технологий возникает зависимость от надежности их оборудования, что может привести к угрозе безопасности как бесперебойной работе, так и к хранимым в облаке данным.

Еще одной угрозой безопасности является доступ к информации ограниченного доступа. Не все данные можно доверить стороннему провайдеру в Интернете, особенно не только для хранения, но и для обработки. Также при применении виртуальной площадки для выполнения лабораторного практикума возникает опасность доступа сторонних лиц к персональным данным обучающихся и интеллектуальному труду разработчика методических рекомендаций для проведения работ [2].

Чтобы решить большинство вышеперечисленных проблем, образовательное учреждение может создать на базе своего оборудования приватное частное облако для организации с применением сертифицированного средства защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальной инфраструктуры на базе систем VMwarevSphere [3]. А в качестве средства защиты информации для виртуальных инфраструктур применить сертифицированное средство, предназначенное для обеспечения безопасности виртуальных инфраструктур на базе платформ VMwarevSphere 4 и 5, применение которого дает возможность легитимной обработки данных ограниченного доступа в виртуальной среде – vGate, имеющее сертификат ФСТЭК России № 2308 от 28 марта 2011 года, действительный до 28 марта 2017года, подтверждающий соответствие vGate требованиям руководящих документов в части защиты от несанкционированного доступа по 5 классу защищенности (СВТ5) и контроля отсутствия недекларированных возможностей по 4 уровню контроля (НДВ4), а также может использоваться в АС до класса защищенности 1Г включительно и для защиты информации в ИСПДн до 1 класса включительно.

При развертывании vGate потребуется выделить только один новый сервер для установки сервера авторизации и, возможно, предусмотреть рабочее место для администратора информационной безопасности. Все остальные компоненты vGate развертываются на базе существующего оборудования виртуальной инфраструктуры (рабочие места АВИ и ESX-серверы). Архитеркура vGate показана на рис. 1.

В vGate реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью. Таким образом, выделяются две основные роли – это администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ).

Доступ на управление виртуальной инфраструктурой или параметрами безопасности предоставляется только аутентифицированным пользователям. Причем процедура аутентификации пользователей и компьютеров (рабочих мест АИБ и АВИ) осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа ManintheMiddle.

Процедура аутентификации АВИ осуществляется с помощью отдельного приложения, которое устанавливается на его рабочее место (агент аутентификации). До соединения с виртуальной инфраструктурой АВИ требуется запустить эту программу и ввести учетные данные.

Для избавления пользователя от многократного ввода имени пользователя и пароля агент аутентификации включает функцию надежного сохранения учетных данных. Эта функция особенно полезна, когда на рабочем месте администратора установлены несколько систем защиты, каждая из которых запрашивает данные для аутентификации.

Для обеспечения защиты средств управления виртуальной инфраструктурой применяется функционал дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Правила разграничения доступа работают на основе заданных ACL и параметров соединения (протоколов, портов). Также в vGate при разграничении прав доступа администраторов виртуальной инфраструктуры к объектам инфраструктуры используется мандатный принцип контроля доступа. Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами подписывается, тем самым обеспечивается защита от атак типа ManintheMiddle в процессе сетевого взаимодействия.

В vGate механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым обеспечивается защита средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины.

Также с помощью данного программного продукта можно обеспечить контроль целостности настроек виртуальных машин перед их загрузкой. Контроль осуществляется

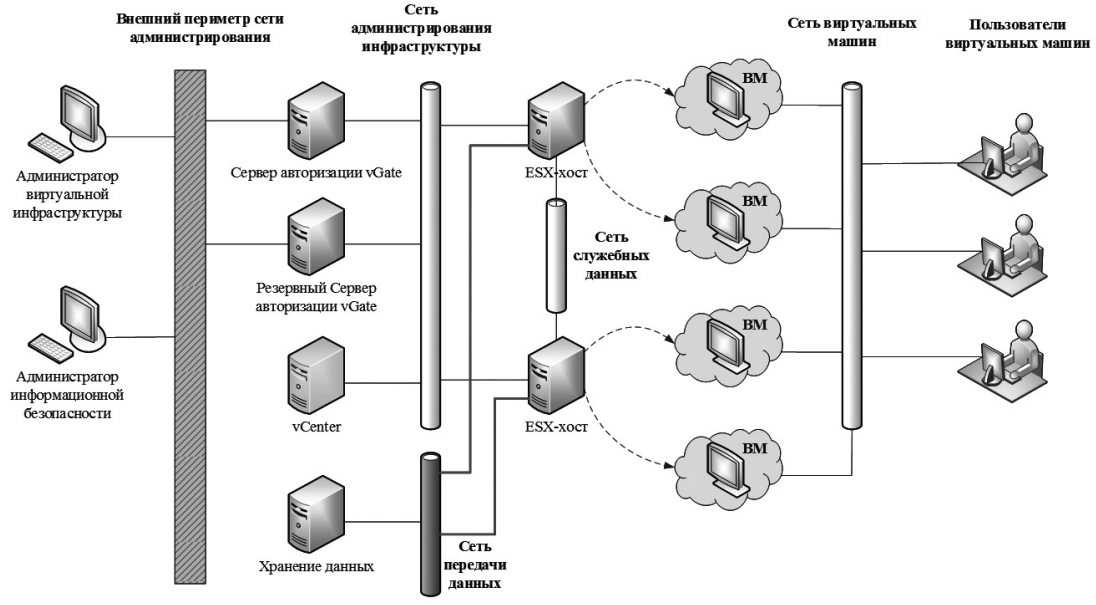

Рис. 1. Архитектура безопасной виртуализации vGate

над файлом *.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров.

Помимо этого осуществляется контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ контролирует целостность файла *.nvram, в котором содержится образ BIOS виртуальной машины.

Доверенная загрузка ОС осуществляется путем контроля целостности загрузочного сектора виртуального диска *.vmdk.

При работе в незащищенной виртуальной инфраструктуре на базе систем VMware администратор этой инфраструктуры обычно может получить доступ к файлам виртуальных машин. Администратор может прямо из VI клиента скачать файл виртуальной машины на локальный диск своего компьютера и исследовать его содержимое. В vGate реализован механизм, позволяющий этот доступ ограничить.

Консоль управления, входящая в состав СЗИ, устанавливается на рабочее место администратора информационной безопасности и позволяет осуществлять мониторинг системы, управлять правами доступа к защищаемым объектам, управлять параметрами виртуальных машин и осуществлять иные функции, связанные с безопасностью системы.

Все изменения, произведенные администратором информационной безопасности, сохраняются централизованно на сервере авторизации.

На рисунке 1 предусмотрено разделение прав на управление виртуальной инфраструктурой и на управление безопасностью. Для этого выделяются две основные роли: администратор виртуальной инфраструктуры и администратор информационной безопасности. Сервер авторизации vGate защищает периметр сети администрирования и разграничивает доступ к серверам виртуализации и к средствам управления виртуальной инфраструктуры. Также для улучшения отказоустойчивости в системе предусмотрел резервный сервер авторизации. При этом сеть администрирования отделяется от остальных сетей виртуальной инфраструктуры.

Ряд компонентов vGate развертывается непосредственно на серверах виртуализации. Это требуется для обеспечения доверенной загрузки виртуальных машин и ряда других функций защиты.

Сеть виртуальных машин отделяется от остальных сетей виртуальной инфраструктуры. При необходимости сеть виртуальных машин может быть фрагментирована.

Данная технология позволяет на базе собственного оборудования университета развернуть безопасную облачную инфраструктуру, где можно реализовать задания, связанные с изучением информационных сетей и их защитой, а также с безопасностью хранения данных и т. д.

Примечания

1. Гузенкова Е. А., Верхорубова Н. А. Обеспечение оптимизации образовательного процесса за счет использования облачных технологий / Перспективы развития информационных технологий: сборник материалов XVIII междунар. науч.-практическ. конференции. – Новосибирск: ЦНРС, 2014. – С. 108–113.

2. Бирюков А. П. Безопасность -2014: облачная и мобильная. // ИнформКурьер-Связь – 2014. № 10 (43). – С. 4–7.

3. Кусек К., Ван Ной В., Дэниел А. Администрирование VMwarevSphere 5: [пер. с англ.]. – СПб. : Питер, 2013. – 381 с.

Гузенкова Елена Алексеевна, ассистент кафедры «Информационные технологии и защита информации». Уральский государственный университет путей сообщения. E-mail: eguzenkova@usurt.ru

Guzenkova Elena, Assistant of the Department «Information technologies and information protection». Ural State University of Railway Transport, Ekaterinburg. E-mail: eguzenkova@usurt.ru

УДК 004.7.056 + 621.396.6 : 621.391.82 + 621.317.08 : 621.396

Антясов И. С., Соколов А. Н.

ОСОБЕННОСТИ ПОСТРОЕНИЯ ЭКРАНИРОВАННЫХ ПОМЕЩЕНИЙ ДЛЯ ИССЛЕДОВАНИЯ СВОЙСТВ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ

В статье рассмотрены проблемы построения и особенности испытаний альтернативных измерительных площадок для проведения специальных исследований технических средств. Приведены определяющие параметры, предъявляемые к безэховым камерам (БЭК), которые влияют на применяемые материалы, форму и размеры площадки. Описаны способы по улучшению характеристик БЭК за счет изменения формы, геометрических особенностей. Представлен метод геометрической оптики для исследований переотражений внутри БЭК.

Ключевые слова: *технический канал утечки информации, специальные исследования, побочные электромагнитные излучения и наводки, электромагнитное поле, безэховая камера, радиопоглощающий материал, безэховая зона, диаграмма направленности.*

Antyasov I. S., Sokolov A. N.

FEATURES CONSTRUCTION SHIELDED ROOM TO STUDY THE PROPERTIES OF ELECTROMAGNETIC FIELD

The problems of construction and testing of alternative features measuring sites for special research techniques. Presents key parameters to be met by an anechoic chamber (BEC), which affect the materials used, the shape and dimensions of the site. The methods to improve the characteristics of BEC by changing the shape of geometric features. The method of geometrical optics research reflections inside the BEC.

Keywords: *technical channel leakage of information, specific studies, side electromagnetic radiation and crosstalk, electromagnetic field, anechoic chamber, radio-absorbing material anechoic area, the radiation pattern.*

Для проведения стендовых специальных исследований (СИ) побочных электромагнитных излучений и наводок (ПЭМИН) в соответствии с нормативно-методическими документами необходимо наличие альтернативной измерительной площадки (АИП). АИП является своего рода безэховой камерой (БЭК), но, если быть точнее, то «полубезэховой» камерой. БЭК называют помещение, облицованное изнутри радиопоглощающим материалом

(РПМ) с целью уменьшения отражения от стен и обеспечения в некотором объеме камеры – безэховой зоне – заданного малого уровня отражений, т. е. условий, приближающихся к условиям «свободного пространства» [1].

Необходимо заметить, что в большинстве современных БЭК гарантированный малый уровень отраженного сигнала или коэффициент безэховости обеспечивается не во всем объеме БЭК, а лишь в ее части, называемой «чистой» или безэховой зоной. [1] В некоторых источниках встречается упоминание данного термина в формулировке «рабочий объем».

В зависимости от типа планируемых измерений предъявляются различные требования к БЭК по форме, размерам, размерам безэховой зоны, коэффициенту безэховости и эффективности экранирования внешних индустриальных радиопомех.

Интересным в практическом отношении диапазоном частот является диапазон от десятков кГц до одного – двух ГГц, в котором сосредоточены основные ПЭМИ от большинства технических средств (ТС), подвергаемых СИ. Но требования ГОСТа [2] предъявляются только к диапазону частот от 30 МГц до 1 ГГц, поэтому целесообразно провести экстраполяцию значений эффективности экранирования до интересующих частот.

Существует целый ряд мероприятий по улучшению характеристик БЭК за счет изменения формы и геометрических особенностей камер. Среди форм можно выделить профилированные с поперечными гофрами, рупорные, камеры с регулируемой торцовой (задней) стенкой, пирамидальные, камеры с криволинейными стенами. Также стоит отметить, что возможно частично облицовывать стены РПМ, если размеры БЭК больше в сравнении с длиной волны. Различные геометрические особенности позволяют добиться многократного переотражения и поглощения электромагнитных волн для уменьшения амплитуды волны. Однако данные БЭК, как правило, имеют существенный недостаток – это сложность перехода на другой диапазон рабочих волн [3], что для проведения СИ является критичным. Поэтому будем рассматривать прямоугольную камеру без применения геометрических методов переотражения за счет формы. При расчетах будем применять метод геометрической оптики, т. е. построение траектории движения лучей электромагнитного поля (ЭМП) внутри камеры с учетом отражения их от стенок камеры. При известных размерах камеры и размерах рабочей зоны возможно выделение нескольких областей: I – наиболее опасная, луч после первого же отражения попадает в рабочий объем, II – луч после второго отражения попадает в рабочий объем, и III – после трех переотражений (рис. 1). Остальные ситуации с большим переотражением менее опасны и реже встречаются в небольших БЭК. Необхо-

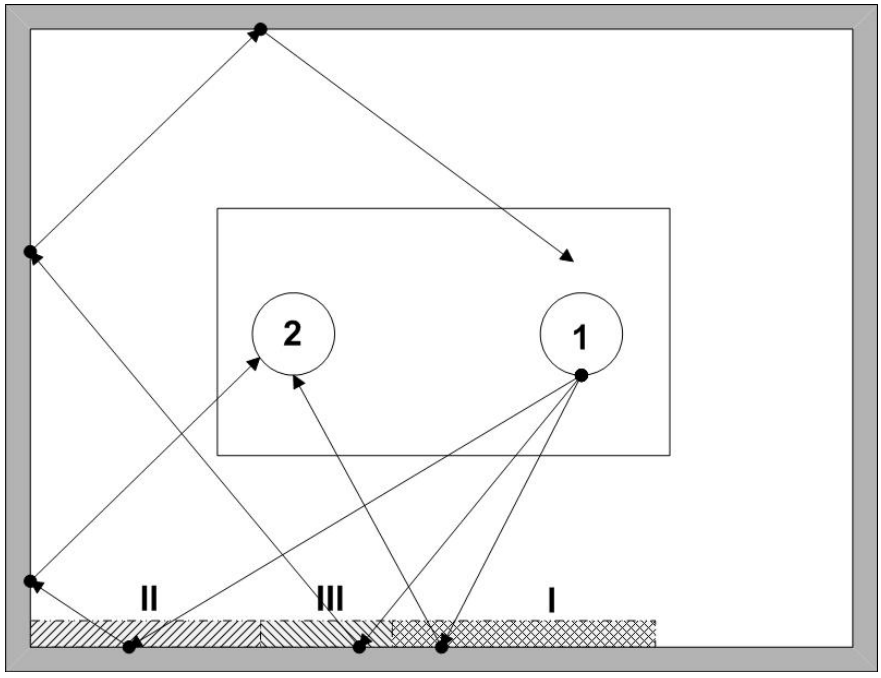

Рис. 1. Области I, II, III с учетом траектории лучей ЭМП в поперечном сечении безэховой камеры

димо также учитывать дифракционные явления на вершинах используемых пирамид или гофров [3].

Определяющими параметрами при построении безэховых камер являются: форма и размеры безэховой зоны, форма и размеры зоны излучения, взаимное расположение зон излучения и безэховости. В нашем случае зоны излучения и безэховости совпадают. При построении БЭК необходимо отталкиваться от габаритов, минимальных для проведения измерений с требуемой точностью, потому что от этого в значительной мере зависит стоимость создания камеры.

Среди методов измерения коэффициента безэховости выделяют [3]:

• метод непосредственного измерения прямого и рассеянного сигналов,

• метод наложения диаграмм направленности (ДН),

• метод перемещающегося индикатора.

Первый метод состоит в измерении в разных точках рабочего объема прямого сигнала и отраженного сигнала с помощью антенн с уменьшенным задним излучением, данный способ не подходит для измерения высококачественных БЭК с хорошим коэффициентом поглощения стенок. Второй метод заключается в измерении ДН приемной антенны в различных точках и их последующем сопоставлении. По расхождениям измеренных ДН можно судить о величине коэффициента безэховости камеры. Последний метод заключается в передвижении приемной антенны вдоль оси и измерении максимального и минимального сигнала, которые сопоставляются со средним значением (сигнал по прямой волне в свободном пространстве). Метод перемещающегося индикатора напрямую используется при оценке коэффициента стоячей волны в соответствии с ГОСТ [4].

Метод испытаний АИП [2] отчасти схож с методом непосредственного измерения прямого и рассеянного сигналов, однако перемещают передающую, а не приемную антенну. Оценка соответствия параметров затухания измерительной площадки определяется как разность между затуханием электромагнитных волн, полученным по результатам экспериментальных исследований на измерительной площадке, и нормированным затуханием электромагнитных волн на измерительной площадке. Перемещение передающей антенны обусловлено имитацией испытуемого ТС при проведении СИ. Необходимо оговорить, что экспериментальное определение затухания АИП проводят для объема, занимаемого испытуемым ТС при его вращении на 360° (рис. 2).

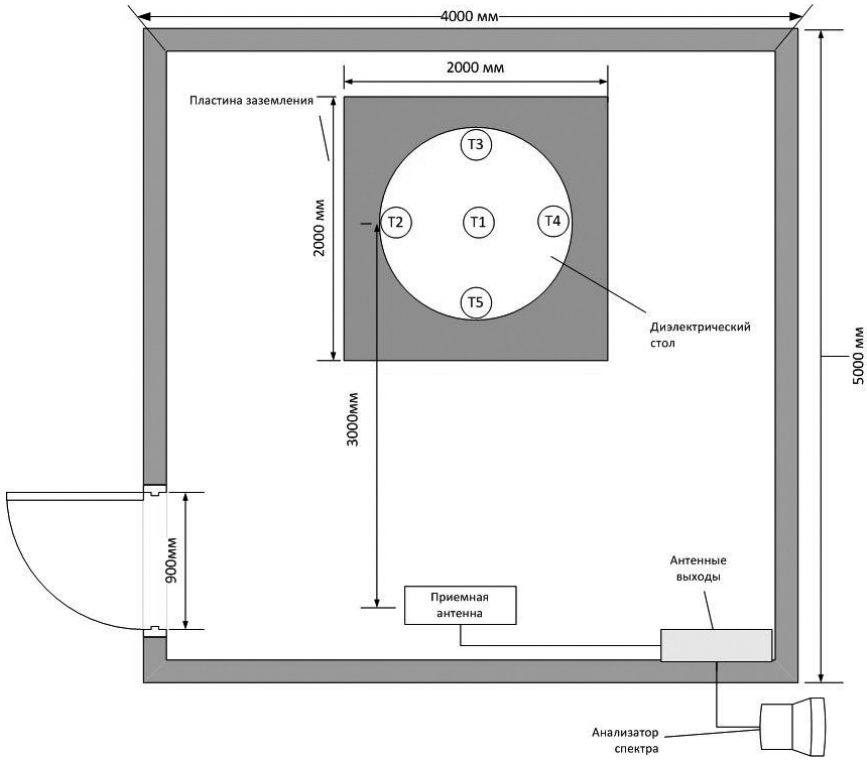

Рис. 2. Схема размещения приемной и передающей антенн при измерениях затуханий, где Т1...Т5 – области размещения передающей антенны

Из практических соображений будем полагать, что испытуемый объем ТС имеет габариты не более 1 х 1,5 х 1,5 м. Минимально допустимым расстоянием при проведении измерений по затуханию является 3 м. С учетом амплитуды перемещения приемной антенны и того, что расстояние от поверхности радиопоглощающего материала до контура испытуемого ТС и антенны должно составлять не менее 1 м, минимальной длиной будет 5 м. Зона безэховости будет представлять собой эллипс и составлять 4,5 х 1,5 м. Минимальная высота будет составлять 3 м, так как необходимо проводить измерения на высоте 1 и 2 м с учетом минимального расстояния от антенны до РПМ. Поперечные размеры АИП будут определяться использованным РПМ, важным параметром которого является максимальный угол падения на поглощающий материал [1].

Важнейшими характеристиками любой БЭК являются эффективности экранирования и поглощения ЭМИ. Данные параметры противоположны друг другу: при усиленном экранировании возникает проблема стоячих волн внутри АИП, а при слабом экранировании внешние индустриальные помехи будут мешать проведению СИ [5].

С целью улучшения коэффициента безэховости применяют РПМ. Все РПМ можно разделить на материалы с электрическим и магнитным поглощением. В требуемом диапазоне будут интересны широкодиапазонные многослойные РПМ с электрическим поглощением. Особенность многослойных состоит в наличии нескольких слоев с различными электрическими потерями в каждом из них, причем потери по мере увеличения толщины материала возрастают. Зачастую такие РПМ имеют форму четырехгранных пирамид (с целью многократного переотражения между их стенками), однако стоит отметить, что эффективность падает при боковом падении ЭМВ.

С целью электромагнитного экранирования широко применяются проволочные сетчатые структуры. Данный выбор обусловлен не только конструктивно-технологическими достоинствами, но и более лучшими характеристиками требуемых климатических условий внутри БЭК. Эффективность электромагнитной защиты при произвольной поляризации источника излучения прежде всего зависит, от густоты сетки и формы ячейки; поэтому, как правило, применяются двумерно-периодические структуры с размерами ячеек, много меньшими длины волны [6].

Таким образом, рассмотрены решения, применяемые при построении БЭК, которые позволяют оптимизировать технические мероприятия и экономические затраты на приведение АИП в соответствие утверждённым нормативам.

Примечания

1. Безэховые камеры СВЧ / М. Ю. Мицмахер, В. А. Торгованов. – М.: Радио и связь, 1982. – 128 с.

2. ГОСТ Р 51320 – 99. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных помех. – Введ. 1999-22-12. – М.: Госстандарт России, 1999. – 27 с.

3. Майзельс Е. Н., Торгованов В. А. Измерение характеристик рассеяния радиолокационных целей. - М.: Сов. радио, 1972. - 232 с.

4. ГОСТ Р 51318.16.1.4 – 2008. Совместимость технических средств электромагнитная. Требования к аппаратуре для измерения параметров индустриальных радиопомех и помехоустойчивости и методы измерений. Часть 1-4. Аппаратура для измерения параметров индустриальных радиопомех и помехоустойчивости. Устройства для измерения излучаемых радиопомех и испытаний на устойчивость к излучаемым радиопомехам.– Введ. 2008-12-25. – М.: Госстандарт России, 2009. – 75 с.

5. Антясов И. С., Соколов А. Н. Особенности валидации альтернативной измерительной площадки для проведения специальных исследований технических средств //Вестник УрФО. Безопасность в информационной сфере. — Челябинск: Изд. центр ЮУрГУ, 2014. — № 1 (11).

6. Электродинамика сетчатых структур / М. И. Конторович, М. И. Астрахан, В. П. Акимов и др. / под ред. М. И. Конторовича. – М.: Радио и связь, 1987. – 136 с.

Антясов Иван Сергеевич, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), г. Челябинск. E-mail: antyasov@gmail.com

Соколов Александр Николаевич, к. т. н., доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), г. Челябинск. E-mail: ANSokolov@inbox.ru

Antyasov Ivan, student of Information Systems Security «South Ural State University», Chelyabinsk. E-mail: antyasov@gmail.com

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security «South Ural State University», Chelyabinsk. E-mail: ANSokolov@inbox.ru

УДК 004.056.53 + 002 : 534.88

Паршин К. А., Анашкин П. А.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ПРЯМЫМ АКУСТИЧЕСКИМ КАНАЛАМ ПРИ АТТЕСТАЦИИ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

Статья посвящена применению альтернативной методики оценки звукоизоляционных свойств помещений, предназначенных для конфиденциальных переговоров. Методика основана на расчете индекса изоляции воздушного шума помещений, носит универсальный характер и может применяться различными организациями, в том числе и коммерческими, так как не требует значительных финансовых затрат и достаточно легко реализуется любым специалистом по защите информации. С целью определения возможности использования методик, применяемых в области охраны труда при оценке шумового воздействия на население, для аудита защищенности помещений при проведении переговоров конфиденциального характера, в статье рассмотрены инструментальная методика оценки защищенности речевой информации от утечки по прямым акустическим каналам при аттестации выделенных помещений, а также расчетно-графическая методика определения индекса звукоизоляции ограждающих конструкций в помещениях, предназначенных для конфиденциальных переговоров. Результатом научной статьи является сравнительный анализ применяемой и альтернативной методики.

Ключевые слова: *звукоизоляционные свойства, индекс изоляции воздушного шума, частотная характеристика, шум, уровень шума, ограждающая конструкция, конфиденциальность.*

Parshin K. A., Anashkin P. A.

COMPARATIVE ANALYSIS OF METHODS OF ASSESSMENT PROTECTED VOICE INFORMATION FROM LEAKING VIA DIRECT ACOUSTIC CHANNEL AT CERTIFICATION OF SELECTED ROOMS

The article is devoted to the use of alternative methods of assessment silenced-relational properties of areas intended for private negotiations. Me-nique is based on the calculation of

the index of airborne sound insulation of premises, is the nature of university-greasy and can be applied by various organizations, including the commer-cal, so it does not require significant financial cost, and easy enough to implement Xia any information security specialists.

In order to determine the possibility of using techniques used in the field of occupational safety, oh when assessing the noise impact on the population, for audit security in premises during the negotiations of a confidential nature, in the article the instrumental method of estimating the security of voice information from leaking via direct-mym acoustic channels space allocated for certification, as well as settlement and graphical method of determining an index of sound insulation of protecting designs in premises designed for confidential talks.

The result of a scientific article is a comparative analysis and applied for alternative techniques.

Keywords: *sound-proof properties, the index of airborne sound insulation, frequency response, noise, noise, cladding, confidentiality, of.*

Оценка звукоизоляционных свойств помещений в целом, и ограждающих конструкций в частности, является одним из важнейших аспектов подготовки помещения к переговорам конфиденциального характера.

Объективные результаты акустической защищенности выделенного помещения дают технические методы контроля. Они различны по сложности, точности измерений и стоимости.

При проведении аттестации соответствующих помещений используется инструментально метод оценки эффективности защиты выделенных помещений от утечки речевой информации [1].

В то же время в области охраны труда и защиты населения от шумового воздействия применяют методики, позволяющие определять уровень изоляции воздушного шума ограждающими конструкциями в жилых и общественных зданиях.

Реализация методик рассмотрена на примере экспериментального помещения, состоящего из следующих ограждающих конструкций:

1) внутренняя перегородка из кирпича толщиной 65 мм (размеры перегородки – 6,0×3,0 м) с одностворчатой двойной с тамбуром деревянной дверью (размеры двери – 2,0×0,9 м);

2) внутренняя перегородка из кирпича толщиной 65 мм (размеры перегородки – 5,0×3,0 м);

3) внешняя стена из кирпича толщиной 140 мм (размеры стены – 6,0×3,0 м) с двумя металлопластиковыми окнами с двухкамерным стеклопакетом (тройным остеклением – 2x150x2x150x2 мм) (размеры окон – 1,2 × 1,8 м);

4) внутренняя перегородка из кирпича толщиной 65 мм (размеры перегородки – 5,0×3,0 м).

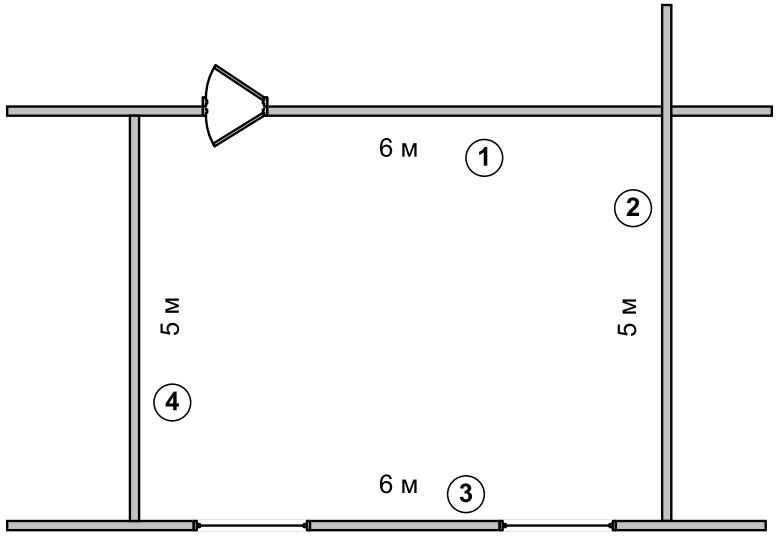

Рис. 1. Экспериментальное помещение

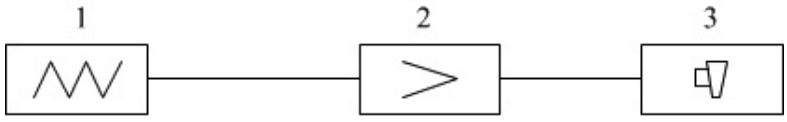

Рис. 2. Аппаратура для создания тестового акустического сигнала:
1 – генератор шума; 2 – усилитель мощности; 3 – акустическая система

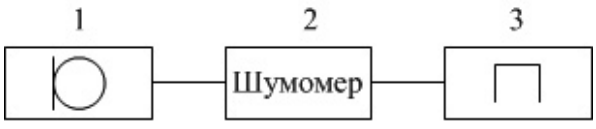

Рис. 3. Аппаратура для измерения звукового сигнала:
1 – измерительный микрофон; 2 – шумомер; 3 – октавные фильтры

Методика оценки защищенности речевой информации от утечки по прямым акустическим каналам при аттестации выделенных помещений [2, 3]

Рассмотрим возможный метод и порядок проведения измерений звукоизолирующей способности ограждающих конструкций защищаемых (выделенных) помещений.

Передающая измерительная система должна содержать: генератор шума; усилители мощности; акустическую систему.

Блок-схема аппаратуры для создания звукового сигнала приведена на рис. 2.

Приемная измерительная система должна содержать: измерительный микрофон; шумомер; третьоктавные полосовые фильтры.

Блок-схема аппаратуры для измерения звукового сигнала приведена на рис. 3.

Порядок проведения измерений и расчетов

Измерительная аппаратура собирается по приведенной на рис. 4 блок-схеме, калибруется и подготавливается к измерениям в соответствии с инструкциями по эксплуатации.

1) Акустическая система (звуковая колонка) источника тестового акустического сигнала устанавливается в месте расположения источника речевого сигнала (высота установки акустической системы над поверхностью пола – 1,5 м). На расстоянии 1 м от акустической системы устанавливается измерительный микрофон. Включается генератор тестового акустического сигнала, устанавливается максимальный уровень излучения и измеряется уровень тестового сигнала для каждой октавной полосы $L_{TC1,i}$. По окончании измерений генератор тестового акустического сигнала выключается, при этом фиксируются его настройки.

2) Измерительный микрофон устанавливается в выбранной контрольной точке на расстоянии r от ограждающей конструкции выделенного помещения до места возможно-

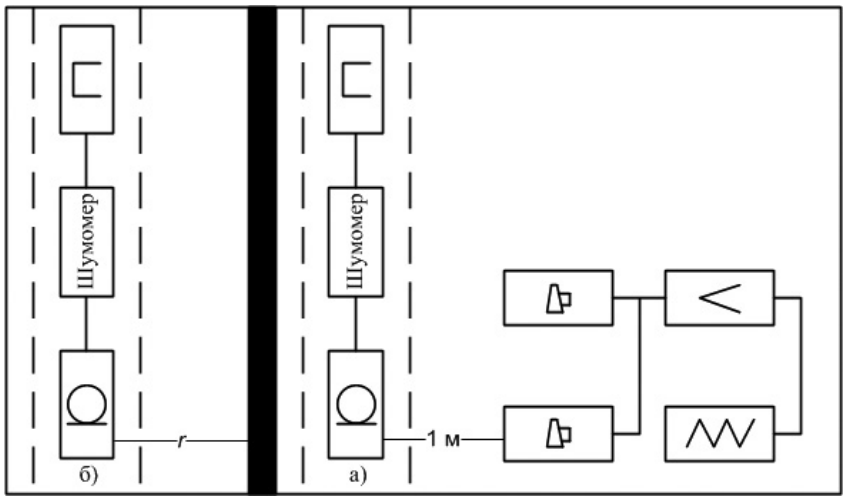

Рис. 4. Схема измерительной установки при контроле выполнения норм защищенности речевой информации:
а) в помещении; б) вне помещения

го размещения средства акустической разведки. Высота установки над поверхностью пола – 1,5 м.

3) При отключенном источнике тестового сигнала шумомером измеряется уровень акустических шумов в контрольной точке в каждой октавной полосе $L_{Ш2.i}$. Измерения проводятся в течение 10–20 минут при отсутствии транспортных шумов и пр. Определяются минимальные значения уровня шумов, полученные при измерениях.

4) Включается генератор тестового акустического сигнала (настройки генератора не изменяются). При включенном источнике тестовых сигналов измеряется уровень суммарного тестового сигнала (сигнал плюс шум) в каждой октавной полосе $L_{ТС2.i}$. Измерения проводятся при отсутствии транспортных шумов.

5) Рассчитывается уровень тестового акустического сигнала в контрольной точке для каждой октавной полосы $L_{ТС.i}$:

$$L_{ТС.i} = 10\lg(10^{0,1L_{ТС2.i}} - 10^{0,1L_{Ш2.i}}), \qquad (1)$$

где $L_{ТС.i}$ – уровень тестового акустического сигнала в контрольной точке в i-й октавной полосе, дБ;

$L_{Ш2.i}$ – уровень акустического шума в контрольной точке в i-й октавной полосе, дБ;

$L_{ТС2.i}$ – уровень тестового суммарного акустического сигнала (сигнал плюс шум) в контрольной точке в i-й октавной полосе, дБ.

6) Рассчитывается затухание акустического сигнала на трассе от места расположения источника речевого сигнала до контрольной точки для каждой октавной полосы Z_i:

$$Z_i = L_{ТС1.i} - L_{ТС.i}, \qquad (2)$$

где Z_i – затухание акустического сигнала на трассе от места расположения источника речевого сигнала до контрольной точки в i-й октавной полосе, дБ;

$L_{ТС1.i}$ – уровень тестового акустического сигнала в выделенном помещении в i-й октавной полосе, дБ.

7) Рассчитывается отношение сигнал/шум в контрольной точке в каждой октавной полосе q_i:

$$q_i = L^*_{С.i} - Z_i - L_{Ш2.i}, \qquad (3)$$

где $L^*_{С.i}$ – уровень скрываемого акустического сигнала в выделенном помещении в i-й октавной полосе, дБ (определяется по табл. 1).

Таблица 1. Типовые уровни речевого сигнала $L^*_{С.i}$, дБ, измеренные в октавных полосах на расстоянии 1 м от источника сигнала в зависимости от вида речи

Номер полосы	Среднегеометрическая частота полосы f_i, Гц	Уровни речевого сигнала $L^*_{С.i}$, дБ, в зависимости от вида речи			
		Тихая речь	Речь средней громкости	Громкая речь	Очень громкая речь
1	125	47	53	59	67
2	250	60	66	72	80
3	500	60	66	72	80
4	1000	55	61	67	75
5	2000	50	56	62	70
6	4000	47	53	59	67
7	8000	43	49	55	63

Полученные результаты измерений в экспериментальном помещении

Таблица 2. Внутренние перегородки из кирпича

i (f_{cpi}), Гц	L_{c1i}, дБ	$L_{ши}$, дБ	$L_{(с+ш)i}$, дБ	L_{c2i}, дБ	Q_i, дБ
1 (250)	91	30	48	48	43
2 (500)	100	30	50	50	50
3 (1000)	96	28	42	42	54
4 (2000)	94	23	43	43	51
5 (4000)	87	17	29	29	58

Таблица 3. Входные двери одностворчатые, деревянные, двойные с тамбуром

i (f_{cpi}), Гц	L_{c1i}, дБ	$L_{ши}$, дБ	$L_{(с+ш)i}$, дБ	L_{c2i}, дБ	Q_i, дБ
1 (250)	88	29	56	56	32
2 (500)	98	24	62	62	36
3 (1000)	94	21	60	60	34
4 (2000)	93	18	64	64	29
5 (4000)	90	15	53	53	37

Таблица 4. Внешняя стена из кирпича

i (f_{cpi}), Гц	L_{c1i}, дБ	$L_{ши}$, дБ	$L_{(с+ш)i}$, дБ	L_{c2i}, дБ	Q_i, дБ
1 (250)	91	30	48	48	43
2 (500)	100	30	50	50	50
3 (1000)	96	28	42	42	54
4 (2000)	94	23	43	43	51
5 (4000)	87	17	29	29	58

Таблица 5. Окна металлопластиковые, с тройным остеклением

i (f_{cpi}), Гц	L_{c1i}, дБ	$L_{ши}$, дБ	$L_{(с+ш)i}$, дБ	L_{c2i}, дБ	Q_i, дБ
1 (250)	88	42	51	50	38
2 (500)	98	38	61	61	37
3 (1000)	94	38	57	57	37
4 (2000)	93	37	55	55	38
5 (4000)	90	38	52	52	38

где i – порядковый номер октавной полосы частот;
f_{cpi} – среднегеометрические частоты октавных полос частот;
$L_{c1i\,i}$ – измеренный уровень тест-сигнала;
$L_{ши}$ – измеренный уровень акустического шума;
$L_{(с+ш)i}$ – уровень измеренного суммарного акустического сигнала и акустического шума;
L_{c2i} – расчетный уровень акустического сигнала;
Q_i – октавные уровни звукоизоляции.

Таким образом, индексы звукоизоляции для данных ограждающих конструкций, полученные инструментальным методом:

1. $R_{К(1)+дверь} = 45$ дБ,
2. $R_{кирп\ (1)} = 50$ дБ,
3. $R_{К(2)+2\ окна} = 42$ дБ,
4. $R_{кирп\ (1)} = 50$ дБ.

Расчетно-графический метод оценки звукоизоляционных свойств помещений, предназначенных для конфиденциальных переговоров

Предлагаемый метод, по сути, является расчетно-графическим, базирующимся на теоретических знаниях о звукоизоляционных свойствах помещений и элементах теории акустики, нормативно закрепленных в СНиП 23-03-2003 «Защита от шума», СП 23-103-2003 «Проектирование звукоизоляции ограждающих конструкций жилых и общественных зданий» [4, 5].

Метод заключается в определении индексов изоляции воздушного шума ограждающими конструкциями на среднегеометрических частотах третьоктавных полос, построении их частотной характеристики и сравнении их с нормируемыми параметрами звукоизоляции ограждающих конструкций помещений. Расчет индекса звукоизоляции ограждающей конструкции производится на основании неблагоприятных отклонений частотной характеристики от нормативной кривой. В итоге делается вывод о возможности обработки информации ограниченного доступа в помещении.

Порядок проведения расчетов

1. Определяем материал и толщину ограждающих конструкций экспериментального помещения.

2. В случае наличия в ограждающих конструкциях дверных и оконных проемов, щелей, отверстий – рассчитываем их площади, а также площади ограждающих конструкций.

3. Звукоизоляцию на среднегеометрических частотах третьоктавных полос каждой из ограждающих конструкций рассчитываем графическим методом [6].

В случае наличия дверных и оконных проемов их звукоизоляция на среднегеометрических частотах третьоктавных полос определяется согласно справочным данным [6].

4. В случае наличия в ограждающих конструкциях дверных и оконных проемов, щелей, отверстий – по формулам (4–5) рассчитываем суммарную звукоизоляцию комбинированных ограждающих конструкций на всех среднегеометрических частотах третьоктавных полос.

Согласно [7], если ограждающая конструкция состоит из нескольких частей с различной звукоизоляцией (например, стена с окном и дверью), изоляцию воздушного шума ограждающей конструкцией R определяют по формуле

$$R = 10\lg\frac{S}{\sum_{i=1}^{n}\frac{S_i}{10^{0,1R_i}}}, \qquad (4)$$

где S_i – площадь i-й части, м^2;
R_i – изоляция воздушного шума i-й частью, дБ.

Если ограждающая конструкция состоит из двух частей с различной звукоизоляцией $(R_1 > R_2)$, R определяют по формуле

$$R = R_1 - 10\lg\frac{\frac{S_1}{S_2} + 10^{0,1(R_1-R_2)}}{1+\frac{S_1}{S_2}}. \qquad (5)$$

5. Строим частотные характеристики ограждающих конструкций, подтверждая точность построения методом интерполяции.

6. Недостающие значения звукоизоляции на среднегеометрических частотах третьоктавных полос определяем графоаналитическим методом по построенным частотным характеристикам.

7. Определяем индекс звукоизоляции каждой ограждающей конструкцией. Для этого рассчитываем сумму неблагоприятных отклонений частотной характеристики ограждающей конструкции от нормативной кривой категории 1.

8. Если сумма неблагоприятных отклонений максимально приближается к 32 дБ, но не превышает эту величину, величина индекса звукоизоляции (R_w) составляет 53 дБ.

Если сумма неблагоприятных отклонений превышает 32 дБ, нормативная кривая смещается вниз на целое число децибел так, чтобы сумма неблагоприятных отклонений не превышала указанную величину.

Если сумма неблагоприятных отклонений значительно меньше 32 дБ или неблагоприятные отклонения отсутствуют, оценочная кривая смещается вверх на целое число

децибел так, чтобы сумма неблагоприятных отклонений от смещенной оценочной кривой максимально приближалась к 32 дБ, но не превышала эту величину.

За величину индекса звукоизоляции принимают ординату смещенной вверх или вниз оценочной кривой в третьоктавной полосе со среднегеометрической частотой 500 Гц.

9. Из полученных значений индексов звукоизоляции каждой ограждающей конструкции выбираем наименьший. Он и будет являться индексом звукоизоляции помещения.

Полученные результаты расчетов в экспериментальном помещении

1. Перегородка из кирпича (65 мм)

$f_{Вкирп(1)}$ = 288 Гц;
$R_{Вкирп(1)}$ = 43 дБ;

Таблица 6. Звукоизоляция перегородки из кирпича толщиной 65 мм (одинарный) на средних частотах третьоктавных полос

Наименование показателя	Средние частоты третьоктавных полос, Гц																
	100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
Изоляция воздушного шума перегородки из кирпича (65 мм) R, дБ	43	43	43	43	43	46	49	51	53	56	58	60	63	64	65	65	65

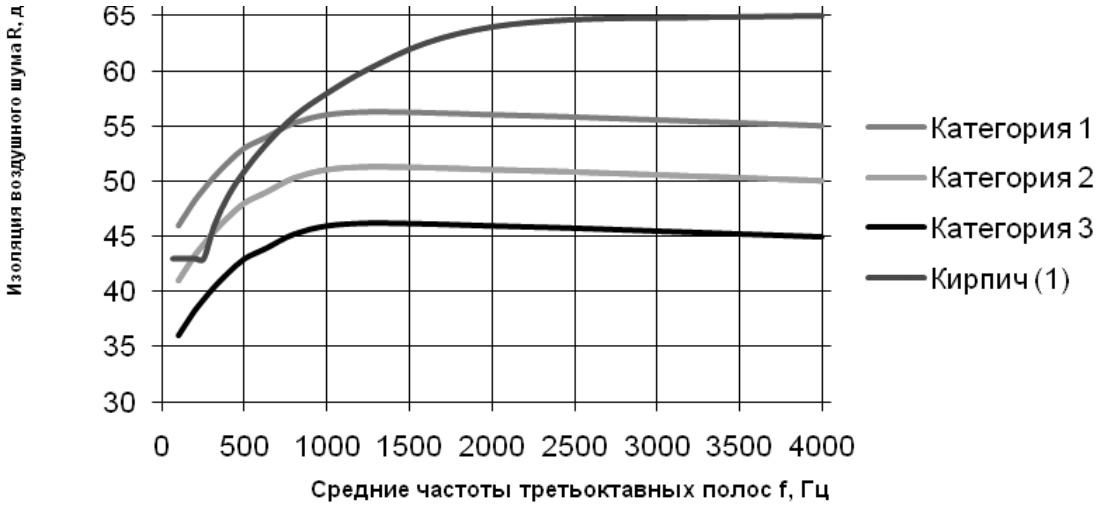

Рис. 5. Частотная характеристика изоляции воздушного шума перегородки из кирпича толщиной 65 мм

Расчет индекса звукоизоляции проводится по форме таблицы 7. Вносим в таблицу значения R оценочной кривой (категория 1) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внутренней перегородки из кирпича толщиной 65 мм (таблица 7). Сумма неблагоприятных отклонений составила 32 дБ, что соответствует требуемому значению в 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_{кирп}$ (1) = 51 дБ.

Таблица 7. Определение индекса звукоизоляции перегородки из кирпича (65 мм)

№ п.п.	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика R (кирпичная перегородка), дБ	43	43	43	43	43	46	49	51	53	56	58	60	63	64	65	65	65
2	Оценочная кривая (1 категория), дБ	46	47	47	48	49	50	52	53	54	55	56	56	56	56	56	55	55
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	3	4	4	5	6	4	3	2	1	-	-	-	-	-	-	-	-
4	Сумма отклонений	$\sum 32 = 32$																
5	Индекс изоляции воздушного шума $R_{кирп(1)}$, дБ								51									

2. Стена из кирпича (140 мм)

$f_{Вкирп(2)}$ = 240 Гц;
$R_{Вкирп(2)}$ = 48 дБ.

Таблица 8. Звукоизоляция стены из кирпича толщиной 140 мм на средних частотах третьоктавных полос

Наименование показателя	Средние частоты третьоктавных полос, Гц																
	100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
Изоляция воздушного шума кирпичной стены (140 мм) R, дБ	48	48	48	48	52	54	57	59	61	63	65	67	69	70	70	70	70

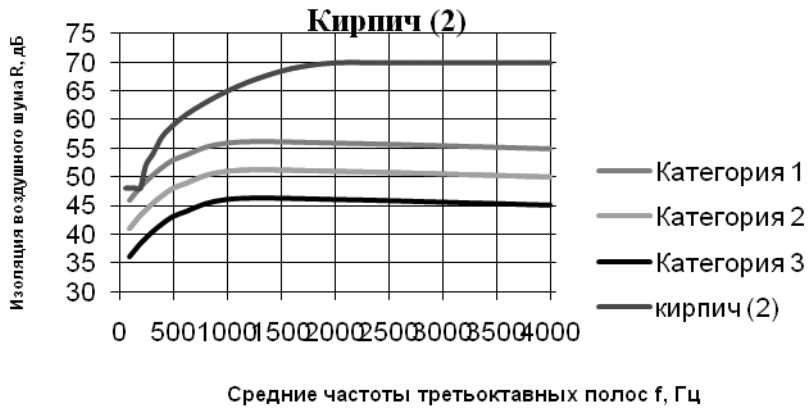

Рис. 6. Частотная характеристика изоляции воздушного шума кирпичной стены толщиной 140 мм

Расчет индекса звукоизоляции проводится по форме таблицы 9. Вносим в таблицу значения R оценочной кривой (категория 1) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внешней стены из кирпича толщиной 140 мм (таблица 9). Сумма неблагоприятных отклонений составила 0 дБ, что меньше требуемого значения в 32 дБ. Смещаем оценочную кривую вверх на 6 дБ и находим сумму неблагоприятных отклонений уже от смещенной оценочной кривой. На этот раз она составляет 26 дБ, что максимально приближается к 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. Rкирп (2) = 59 дБ.

Таблица 9. Определение индекса звукоизоляции внешней стены из кирпича (140 мм)

№ п.п.	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика R (внешней стены из кирпича), дБ	48	48	48	48	52	54	57	59	61	63	65	67	69	70	70	70	70
2	Оценочная кривая (1 категория), дБ	46	47	47	48	49	50	52	53	54	55	56	56	56	56	56	55	55
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	-	-
4	Сумма отклонений	$\sum 0 < 32$																
5	Оценочная кривая, смещенная вверх на 6 дБ	52	53	53	54	55	56	58	59	60	61	62	62	62	62	62	61	61
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	4	5	5	6	3	2	1										
7	Сумма отклонений	$\sum 26 \approx 32$																
8	Индекс изоляции воздушного шума Rкирп (2), дБ								59									

Звукоизоляцию оконных проемов и дверей берем из справочника.

Рассчитываем звукоизоляцию ограждающих конструкций, состоящих из нескольких частей с разной звукоизоляцией:

1) внутренняя перегородка из кирпича толщиной 65 мм (размеры перегородки – 6,0×3,0 м) с одностворчатой двойной с тамбуром деревянной дверью (размеры двери – 2,0×0,9 м);

2) внешняя стена из кирпича толщиной 140 мм (размеры стены – 6,0×3,0 м)) с двумя металлопластиковыми окнами с двухкамерным стеклопакетом (тройным остеклением – 2x150x2x150x2 мм) (размеры окон – 1,2 × 1,8 м);

Рассчитанные данные заносим в табл. 10.

Таблица 10. Звукоизоляция ограждающих конструкций, состоящих из двух частей

Тип	Конструкция	Звукоизоляция R (дБ) на частотах, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1. Внутренняя перегородка из кирпича с одностворчатой двойной с тамбуром деревянной дверью с уплотнителями и без порога	Стена: толщина – 65 мм, высота – 3,0 м, ширина – 6,0 м. Дверь: высота – 2,0 м, ширина – 0,9 м, ширина – 1,2 м.	36	37	38	38	39	40	42	43	44	46	46	45	44	42	42	41	40
2. Внешняя стена из кирпича с двумя металлопластиковыми окнами с двухкамерным стеклопакетом (тройным остеклением – 2x150x2x150x2 мм) с уплотнительными прокладками	Стена: толщина – 140 мм, высота – 3,0 м, ширина –6,0 м. Окна: толщина стекла – 2 мм, возд. промежуток – 150 мм, высота – 1,8 м.	31	31	34	38	42	44	45	47	50	53	56	57	58	59	59	60	61

Построим частотные характеристики для данных ограждающих конструкций (рис. 7).

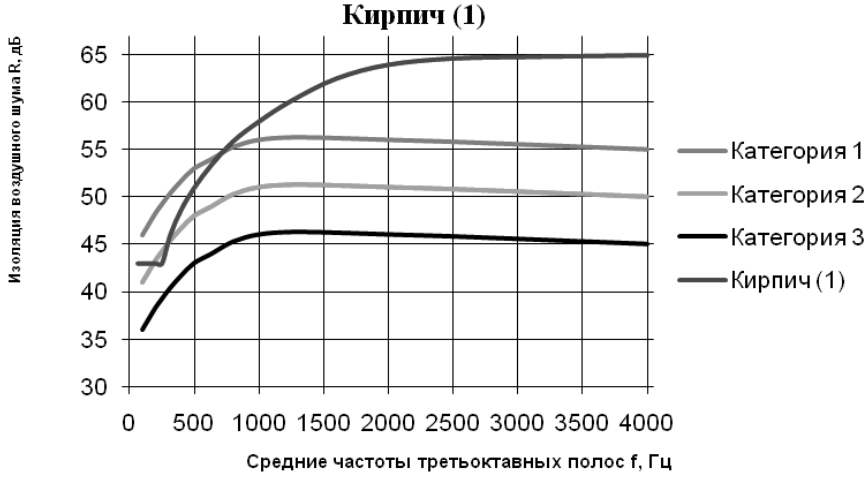

Рис. 7а. Расчетные частотные характеристики.
Частотная характеристика звукоизоляции внутренней перегородки из кирпича (65 мм)

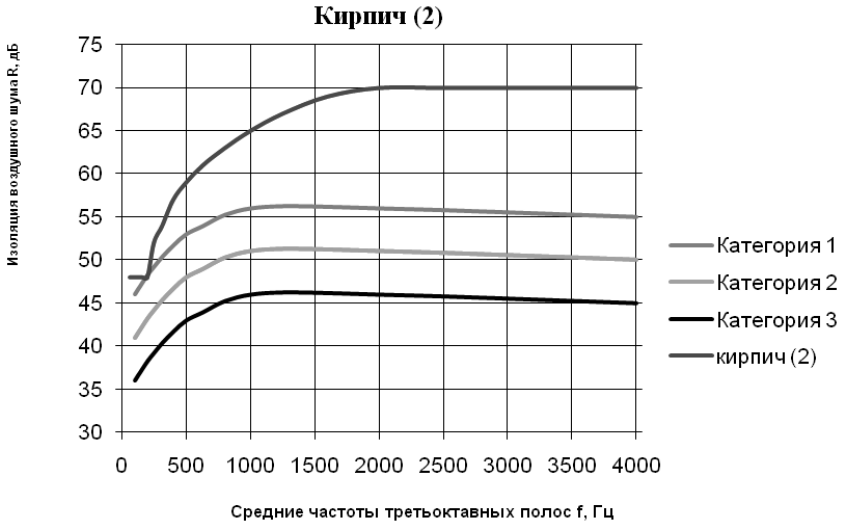

Рис. 7б. Расчетные частотные характеристики.
Частотная характеристика звукоизоляции внешней стены из кирпича (140 мм).

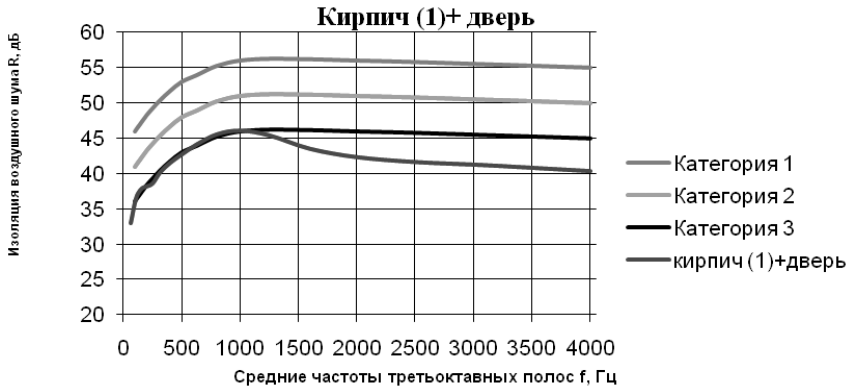

Рис. 7в. Расчетные частотные характеристики.
Частотная характеристика звукоизоляции внутренней перегородки из кирпича толщиной 65 мм (размеры перегородки – 6,0 × 3,0 м) с одностворчатой двойной с тамбуром деревянной дверью с уплотнителями и без порога.

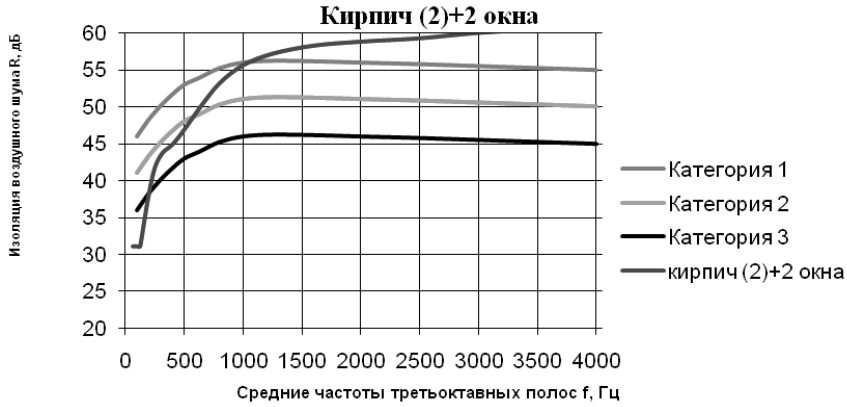

Рис. 7г. Расчетные частотные характеристики.
Частотная характеристика звукоизоляции внешней стены из кирпича толщиной 140 мм (размеры стены – 6,0 × 3,0 м) с двумя металлопластиковыми окнами с двухкамерным стеклопакетом (тройным остеклением – 2x150x2x150x2 мм) с уплотнительными прокладками

Расчет индекса звукоизоляции проводится по форме таблицы 11. Вносим в таблицу значения R оценочной кривой (категория 2) и находим неблагоприятные отклонения расчетной частотной характеристики от оценочной кривой (пункт 3). Средняя величина отклонений должна максимально приближаться к 32 дБ, но не превышать эту величину.

Определим индекс звукоизоляции внутренней перегородки из кирпича толщиной 65 мм с дверью (табл. 11). Сумма неблагоприятных отклонений составила 104 дБ, что превышает требуемое значение в 32 дБ. Смещаем оценочную кривую вниз на 5 дБ и находим сумму неблагоприятных отклонений уже от смещенной оценочной кривой. На этот раз она составляет 20 дБ, что максимально приближается к 32 дБ. За величину индекса изоляции принимаем значение смещенной оценочной кривой в 1/3-октавной полосе 500 Гц, т. е. $R_{К(1)+дверь}$ = 43 дБ.

Таблица 11. Определение индекса звукоизоляции внутренней перегородки из кирпича (размеры перегородки – 6,0×3,0 м) с одностворчатой двойной с тамбуром деревянной дверью с уплотнителями и без порога

№ п.п.	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика R (внутренняя перегородка из кирпича (1) с дверью), дБ	36	37	38	38	39	40	42	43	44	46	46	45	44	42	42	41	40
2	Оценочная кривая (2 категория), дБ	41	42	42	43	44	45	47	48	49	50	51	51	51	51	51	50	50
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	5	4	4	5	6	5	5	5	5	5	5	6	8	9	9	9	10
4	Сумма отклонений	$\sum 104 \gg 32$																
5	Оценочная кривая, смещенная вниз на 5 дБ	36	37	37	38	39	40	42	43	44	45	46	46	46	46	46	45	45
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	0	-	-	0	1	0	0	0	0	0	0	1	3	4	4	4	5
7	Сумма отклонений	$\sum 20 \approx 32$																
8	Индекс изоляции воздушного шума $R_{К(1)+дверь}$, дБ								43									

Аналогично рассчитываем индекс звукоизоляции для остальных ограждений (таблица 12).

Таблица 12. Определение индекса звукоизоляции внешней стены из кирпича толщиной 140 мм (двойной) (размеры стены – 6,0×3,0 м) с двумя металлопластиковыми окнами с двухкамерным стеклопакетом (тройным остеклением – 2х150х2х150х2 мм) с уплотнительными прокладками

№ п.п.	Параметры	Среднегеометрическая частота 1/3-октавной полосы, Гц																
		100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000
1	Расчетная частотная характеристика R (внешняя стена из кирпича (2) с 2-мя окнами), дБ	31	31	34	38	42	44	45	47	50	53	56	57	58	59	59	60	61
2	Оценочная кривая (2 категория), дБ	41	42	42	43	44	45	47	48	49	50	51	51	51	51	51	50	50
3	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	10	10	8	5	2	2	2	1	-	-	-	-	-	-	-	-	-
4	Сумма отклонений	$\sum 40 > 32$																
5	Оценочная кривая, смещенная вниз на 1 дБ	40	41	41	42	43	44	46	47	48	49	50	50	50	50	50	49	49
6	Неблагоприятные отклонения от смещенной оценочной кривой, дБ	9	9	7	4	1	1	1	0	-	-	-	-	-	-	-	-	-
7	Сумма отклонений	$\sum 32 = 32$																
8	Индекс изоляции воздушного шума $R_{K(2)+2\ окна}$, дБ								47									

Таким образом, индексы звукоизоляции для данных ограждающих конструкций:

$R_{K(1)+дверь}$ = **43 дБ,**
$R_{кирп\ (1)}$ = 51 дБ,
$R_{K(2)+2\ окна}$ = 47 дБ,
$R_{кирп\ (1)}$ = 51 дБ.

Из полученных значений индексов звукоизоляции каждой ограждающей конструкции выбираем наименьший. Он и будет являться индексом звукоизоляции помещения, т. е. индекс звукоизоляции экспериментального помещения – 43 дБ.

Анализ результатов

Таблица 13. Анализ результатов

Помещение	Звукоизоляция, дБ	
	Расчетно-графический метод	Инструментальный метод
Экспериментальное помещение	43	42

Эксперимент показал, что разработанная расчетно-графическая методика применима для определения звукоизоляции помещений, исходя из характеристик и звукоизоляционных свойств ограждающих конструкций, что подтверждается корреляцией проведенных расчетов и замеров. Применение расчетно-графической методики не требует значительных финансовых затрат и достаточно легко реализуется любым специалистом по защите информации.

Примечания:

1. Хорев А. А. Контроль эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам // Защита информации. Инсайд. 2010. № 1. С. 34–45.

2. Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4. С. 39–45.

3. Дворянкин С. В., Макаров Ю. К., Хорев А. А. Обоснование критериев эффективности защиты речевой информации // Защита информации. Инсайд. 2007. № 2. С. 18–25.

4. СНиП 23-03-2003 «Защита от шума». М.: Госстрой России, ФГУП ЦПП, 2004.

5. СП 23-103-2003 «Проектирование звукоизоляции ограждающих конструкций жилых и общественных зданий». М.: Госстрой России, ФГУП ЦПП, 2004.

6. Технология защиты речевой информации в помещениях: учеб.-методич. пособие. К. А. Паршин, А. А. Копылова. – Екатеринбург: УрГУПС, 2010. – 88 с.

7. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам: учеб. пособие. М.: Горячая линия – Телеком, 2005. –416 с

8. Паршин К. А., Анашкин П. А. О применении методов оценки шумового воздействия на население при защите речевой информации // Вестник Уральского государственного университета путей сообщения. 2013. № 2. с. 45–53.

Паршин Константин Анатольевич, к. т. н, доцент кафедры «Информационные технологии и защита информации» УрГУПС, Екатеринбург. E-mail: KParshin@usurt.ru

Анашкин Павел Анатольевич, генеральный директор, ОАО «Уралгеоинформ», УрГУПС, Екатеринбург. E-mail: v060138@gmail.com

Konstantin Parshin, associate professor of « Information technologies and protection of information « Ural State University of Railway Transport , Ekaterinburg. E-mail: KParshin@usurt.ru

Pavel Anashkin, General Director, JSC «Uralgeoinform», Ural State University of Railway Transport, Ekaterinburg. E-mail: v060138@gmail.com

УДК 004.7.056.53

Асяев Г. Д., Никольская К. Ю.

АТАКИ НА КАНАЛЬНЫЙ УРОВЕНЬ

С развитием постиндустриального общества развиваются и информационные технологии, следовательно, учащаются атаки на эти технологии. Сетевая отрасль занимает лидирующую позицию по количеству атак. В модели OSI будем брать канальный уровень, так как на этом уровне основной опасностью является то, что, взломав сеть, тот, кто атакует, может пройти через средства защиты более высоких уровней. В данной статье рассматриваются несколько видов атак на канальном уровне, например, такие как перехват трафика. Также рассматриваются основные принципы построения безопасности в России. Рассмотрена законодательная база в сфере информационной безопасности.

Ключевые слова: *канальный уровень, модель OSI, виды атак, безопасность.*

Asyaev G. D., Nikolskaya K. U.

ATTACKS ON THE DATA LINK LAYER

With the development of post-industrial society. Developing information technologies and, consequently, more frequent attacks on these technologies. Network industry is a leader in the number of attacks. The OSI model will take the data link layer. Since at this level, the main risk is that the hacking network, the one who attacks can pass through the higher levels of protection. This article discusses several types of attacks on the data link layer, for example, such as the interception of traffic. It also discusses the basic principles of safety in Russia. We consider the legal framework in the field of information security.

Keywords: *Link Layer Model OSI, types of attacks, security.*

Модель OSI представляет собой семиуровневую систему. Это физический, канальный, сетевой, транспортный, сеансовый, представительный, прикладной уровень. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями и использует протоколы. Протоколы – это стандарты, определяющие формы представления и способы пересылки сообщений, процедуры их интерпретации, правила совместной работы различного оборудования в сетях.

Рассмотрим основной принцип функционирования и функции канального уровня. Для этого перенесёмся на физический уровень. Там передаются только биты. И, к сожалению, не учитывается, что физическая среда для передачи может быть занята, из-за чего возникают ошибки. Именно для этого на канальном уровне осуществляется проверка доступности среды передачи, а также обнаружение и устранение ошибок. В глобальных же сетях канальный уровень обеспечивает

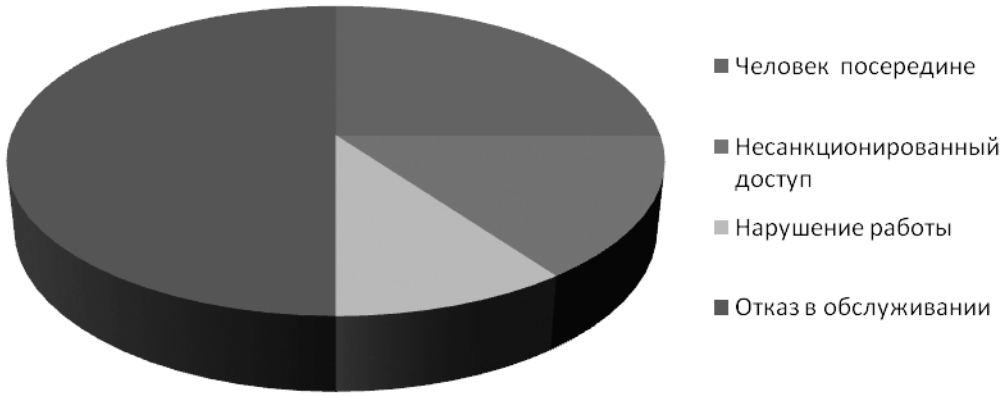

Рис. 1. Частота использования типов атак на канальном уровне

обмен сообщениями между соседними компьютерами. Так канальный уровень можно понимать как локальную сеть. Именно поэтому стоит обеспечить максимальную безопасность. В соответствии с Федеральным законом «О безопасности» [1] основными принципами обеспечения безопасности являются:

1. Соблюдение и защита прав и свобод человека и гражданина;
2. Законность;
3. Системность и комплексность;
4. Приоритет предупредительных мер в целях обеспечения безопасности;
5. Взаимодействие федеральных органов государственной власти.

Атаки на канальном уровне очень распространены. Как правило, предполагается, что тот, кто атакует, находит в локальной сети, либо есть какое-то связующее звено.

Атаки на канальный уровень подразделяются на такие типы, как:

- Несанкционированный доступ к сети либо к её участкам;
- Отказ в обслуживании (DoS);
- «Человек посередине» (Man in the middle);
- Нарушение работы сети (Disruption of the network);
- Воздействия на тело кадра (внесение ошибок, подмена, потеря и имитация);
- Воздействия на оборудование звена передачи данных;
- Попытки несанкционированного доступа к средствам криптографической защиты информации канального уровня.

Рассмотрим поподробнее эти атаки.

Несанкционированный доступ к сети. Основной принцип заключается в том, чтобы найти и использовать недостатки протоколов. В том числе путём воздействия на тело кадра, а именно: внесение ошибок, подмена, потеря, тем самым всеми этими действиями получая доступ к участкам сети. [2]

Отказ в обслуживании. Один из самых распространённых типов атак. Основная суть состоит в том, что взять какой-либо ресурс системы и частыми запросами довести его до отказа. Кроме того, на канальном уровне есть определённый тип атак, с помощью которых можно получить односторонний доступ. Одним из наиболее часто используемых способов нападения на канальный уровень является управление разнесенными антеннами. Допустим: есть точка доступа, называемая AP, с разнесенными антеннами A (для левой стороны) и B (соответственно для правой). Если пользователи I и II находятся на разных сторонах офиса, то каждый из них по умолчанию обращается к различным антеннам на точке доступа. Здесь возникает проблема: если пользователь I решит имитировать MAC адрес пользователя II, увеличивая силу его сигнала, чтобы по крайней мере уравнять и при этом не превысить силу сигнала пользователя II на антенне B, точка доступа больше не будет принимать или посылать данные от пользователя II, что свидетельствует об успешной атаке.

Другой проблемой на канальном уровне беспроводных сетей является spoofing точек доступа. Зададимся вопросом в контексте сетевой безопасности: spoofing attack понимается как ситуация, в которой один человек или программа успешно маскируется под другую путем фальсификации данных и позволяет получить незаконные преимущества. Клиентская часть обычно конфигурируется таким образом, чтобы связываться с

точкой доступа с наиболее сильным сигналом. Нападавший может просто подделывать название точки доступа, и клиенты автоматически будут с ней связываться. Таким образом, злоумышленник может захватывать весь трафик.

Нарушение работы. Без сомнений, протокол содержит какие-либо ошибки или недостатки. Суть данной атаки – это найти эти недостатки и нарушить их нормальную работу и, как следствие, нарушить работу всей сети

Человек посередине. Суть: предполагает наличие человека, который прослушивает трафик или подменяет его. Перехват трафика, в свою очередь, может осуществляться:

1) обычным «прослушиванием» сетевого интерфейса;

2) подключением сниффера в разрыв канала. Под сниффером стоит понимать сетевой анализатор трафика, программу или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов;

3) ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер.

Для того чтобы предотвратить атаку такого типа, нужно провести шифрование данных на различных уровнях. В противном случае большие объемы передаваемой конфиденциальной информации будут попадать к злоумышленникам для дальнейшего использования (в том числе и в коммерческих целях).

Тем самым канальный уровень выполняет функции логической организации передачи данных через физический уровень. Отсюда следует, что канальный уровень – достаточно уязвлённое место. А с ростом информатизации количество атак становится всё больше и больше. Рассматривая уже существующие типы атак, следует особое внимание уделить такому типу, как «Человек посередине» и Отказ в обслуживании.

Примечания

1. Федеральный закон о безопасности.
2. https://ru.wikipedia.org/wiki/%CA%E0%ED%E0%EB%FC%ED%FB%E9_%F3%F0%EE%E2%E5%ED%FC
3. http://www.on-lan.ru/ch9-5.html

Асяев Григорий Дмитриевич, студент КТУР-171 ЮУрГУ, г. Челябинск. E-mail: asyaev1996@mail.ru

Никольская Ксения Юрьевна, преподаватель кафедры «Безопасность информационных систем ЮУрГУ», г. Челябинск. E-mail: bambucha13@mail.ru

Asyaev Gregory, student SUSU, Chelyabinsk. E-mail: asyaev1996@mail.ru

Nikolskaya Ksenia, Lecturer, Department of Information Systems Security SUSU, Chelyabinsk. E-mail: bambucha13@mail.ru

УДК 738.5.057.4 : 003.27 + 004.738.2 : 003.27

Токарчук Н. А., Середкина Е. Д., Зюляркина Н. Д.

ИССЛЕДОВАНИЕ ПРОТОКОЛА TCP ДЛЯ ПЕРЕДАЧИ СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ

В данной статье рассмотрено создание модулей Netfilter ядра linux для скрытой передачи сообщений через сеть Интернет на основе использования протокола TCP. Также в рамках работы решаются такие задачи, как контроль потоков сообщений к различным адресатам и взаимодействие между пользователем и модулями. Мы предлагаем вместо изменения исходного кода ядра Linux использовать динамически подключаемые модули Netfilter. Использование модулей Netfilter позволяет перехватывать любые пакеты при отправке и приеме, а также изменять их любым способом. В рамках данной работы было создано два модуля Netfilter: модуль отправки и модуль приема сообщений. Данные модули могут подключаться через стандартный механизм регистрации модулей на любом компьютере с системой Linux.

Ключевые слова: *стеганография, netfilter, tcp, linux.*

Tokarczuk N. A., Seredkina E. D., Zyulyarkina N. D.

STUDY OF TCP FOR TRANSMISSION STEGANOGRAPHIC MESSAGES

This article discusses the creation of Netfilter kernel modules linux flush message transmission via the Internet through the use of protocol TCP. Also in the framework of the solved tasks such as flow control messages to various destinations, and the interaction between the user and modules. We offer instead of changing the source code of the Linux kernel to use plug-ins dynamically Netfilter. Using Netfilter module allows you to capture any packets for sending and receiving, as well as to change them in any way. As part of this work was created two modules Netfilter: sending module and the module receiving messages. These modules can be connected via a standard mechanism for the registration module on any computer system Linux.vzaimodeystvuet with the protected program, the learning process is called a process of reverse (reverse) engineering. This process often depends on the properties of the human psyche, so the use of these properties can reduce the efficiency of the process of reverse engineering. Obfuscation ("obfuscation" - trapping), is one of the methods to protect code that allows you to complicate the process of reverse engineering of code protected software. Obfuscation could be applied not only to protect the PP, it has wider application, for example it may be used creators of viruses to protect their creations, etc.

Keywords: *steganography, netfilter, tcp, linux.*

В статье «Протокол TCP как стеганографический контейнер» [1] мы рассматривали способ изменения исходного кода ядра Linux для передачи стеганографических сообщений с помощью протокола TCP. В данной работе мы предлагаем вместо изменения исходного кода ядра Linux использовать динамически подключаемые модули Netfilter. Использование модулей Netfilter позволяет перехватывать любые пакеты при отправке и приеме, а также изменять их любым способом.

В рамках данной работы было создано два модуля Netfilter: модуль отправки и модуль приема сообщений. Данные модули могут подключаться через стандартный механизм регистрации модулей на любом компьютере с системой Linux (kernel 3.x и выше).

Отправка сообщений

Модуль отправки сообщений перехватывает созданные локальным компьютером TCP сегменты в точке перехвата NF_INET_LOCAL_OUT. Перехваченный сегмент TCP с некоторым шансом заменяется на сообщение, которое требует скрытой передачи. В результате замены данных в сегменте контрольная сумма становится неверной. Если длина поля данных сегмента меньше, чем сообщение, которое нужно передать, то это сообщение обрезается до нужной длины, а оставшаяся часть отправляется при следующей скрытой передаче.

Принимающая сторона из-за не прошедшей проверку контрольной суммы не присылает подтверждение ACK для данного сегмента. Согласно механизму RTO, отправитель должен переслать сообщение, на которое он не получил ACK подтверждение. В момент повторной отправки сегмента адресату, сообщение изменяется на исходное, и ему восстанавливается контрольная сумма. Данный механизм позволяет паразитировать на любом трафике, идущем от отправителя к получателю.

Прием сообщений

Модуль приема сообщения ловит сегменты в точке перехвата NF_INET_LOCAL_IN. По умолчанию считается, что все сегменты с некорректной контрольной суммой – это стеганографические сообщения. Каждый такой сегмент далее проходит проверку. Стеганографическое сообщение содержит в себе внутреннюю контрольную сумму, через соответствие которой и можно судить, настоящее ли это стеганографическое сообщение.

Контроль потоков

В нашей работе мы используем перехват сегментов на сетевом уровне, поэтому мы должны сами контролировать, кому отправлять сообщения. Для отправки сообщений нескольким адресатам был организован контроль потоков сообщений. При отправке сегмента проверяется, есть ли для адреса назначения буфер со стеганографическими сообщениями, и замена данных в сегменте происходит только из нужного буфера. Если же буфер отсутствует, то сегменты всегда остаются неизменными.

Взаимодействие модулей с пользователем

Чтобы добавить сообщение в буфер, необходимо передать модулю сообщение и IP-адрес назначения.

Для того чтобы модуль мог преобразовать переданные ему данные, создана вспомогательная утилита StegFormat, которая преобразует строку вида «<сообщение> <ip-адрес>» в строку, которую может распознать модуль. IP-адрес преобразуется функцией inet_addr, содержащейся в заголовочном файле arpa/inet.h.

Преобразованная строка передается модулю с помощью виртуальной файловой системы /proc. Данная файловая система располагается в памяти и позволяет взаимодействовать с процессами ядра Linux. Самый простой пример: чтобы передать информацию, достаточно выполнить команду «echo «сообщение» > /proc/<название модуля>».

При выполнении данной команды модуль регистрирует запись в него и вызывает функцию write_new_message(), которая добавляет новое сообщение в необходимый поток на основе IP-адреса.

Описанный метод передачи не является абсолютно надежным для передачи сообщений, так как если направленно просматривать трафик жертвы, то программы анализа трафика (например, Wireshark) отображают данные сообщения в открытом виде. Однако если трафика от отправителя к получателю много, а процент скрытых сообщений достаточно мал, отследить такое сообщение при незнании способа скрытой передачи может быть достаточно сложной задачей. Для того чтобы повысить надежность данного метода, можно использовать принудительное шифрование данных.

Примечания

1. Токарчук, Н. А. Протокол TCP как стеганографический контейнер [текст]/ Н. А. Токарчук, Е. Д. Середкина, Н. Д. Зюляркина //Вестник УрФО Безопасность в информационной сфере / Издательский центр ЮУрГУ – Челябинск, 2014 – Вып. 4(14) – С. 36–39.

Токарчук Никита Александрович, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). Email: personal@mainnika.ru

Зюляркина Наталья Дмитриевна, кандидат физ.-мат. наук, доцент, преподаватель кафедры «Безопасность информационных систем», г. Челябинск. E-mail: toddeath@yandex.ru

Tokarczuk Nikita, students of the department of information systems security «South Ural State University». Email: personal@mainnika.ru

Zyulyarkina Natalia, Candidate of Physics and Mathematics, Associate Professor, Lecturer, Department of Information Systems Security, Chelyabinsk. E-mail: toddeath@yandex.ru

УДК 004.451.056.53

Окороков В. А.

ЗАЩИЩЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Рассмотрена роль операционных систем (ОС) в организации систем защиты информации. Перечислены основные требования и механизмы, которые необходимо реализовать в рамках операционной системы для обеспечения надежной защиты данных. Изучена возможность применения ОС Astra Linux в качестве базовой ОС, предназначенной для использования в учебном процессе по направлению «Информационная безопасность».

Ключевые слова: *информация, безопасность, операционные системы, защита данных, обучение.*

Okorokov V. A.

SECURE OPERATING SYSTEM

The role of the operating system (OS) in the organization of information security systems. The basic requirements and mechanisms to be implemented within the operating system to ensure reliable data protection. The possibility of using the OS Astra Linux as the base OS for use in the educational process in the direction of "Information Security".

Keywords: *information, security, operating systems, data protection, training.*

Проблема обеспечения информационной безопасности носит комплексный характер и для ее решения требуется разработка организационных и технических мер, которые должны поддерживаться в рамках любой организации, связанной с использованием информационных систем.

Базовым подходом к обеспечению информационной безопасности является ограничение доступа субъектов информационных отношений к данным. Меры по разграничению доступа могут быть эффективны только в том случае, если внутри предприятия существует и исполняется некоторая политика, определяющая порядок доступа пользователей к данным. В рамках политики безопасности необходимо для каждого субъекта определить разрешенные объекты данных и методы доступа к ним.

Реализация политики ограничения доступа в рамках информационной системы невозможна без применения программно-технических средств, позволяющих определить, имеет ли право определенный пользователь получать требуемый вид доступа к заданным объектам данных. Если соответствующие программные компоненты находятся в привилегированном положении по отношению к программам пользователя, то это существенно усложняет их модификацию или подмену. Единственной программой, которая работает в привилегированном режиме, является операционная система. Поэтому именно операционная система должна нести ответственность за поддержку основных механизмов, обеспечивающих реализацию политики безопасности [6].

Базовые механизмы

Детали политики безопасности организации могут существенно изменяться с течением времени. Соответствующие изменения операционной системы не всегда возможны. Поэтому программно-технические средства поддержки безопасности разумно разделить на две группы [1].

К первой группе относятся базовые механизмы безопасности, которые требуют привилегированного доступа к системным ресурсам. Базовые механизмы обычно реализуются в виде модулей операционной системы, работающих в режиме ядра и использующих системные структуры данных, также находящиеся в области памяти ядра.

Ко второй группе относятся детальные механизмы ограничения доступа, реализующие текущую политику безопасности, принятую в организации. Поддержка таких механизмов выполняется с помощью программ пользовательского уровня, что позволяет относительно легко их модифицировать в соответствии с новыми требованиями. Программы пользовательского уровня, предназначенные для реализации политики безопасности, должны иметь доступ к базовым механизмам безопасности операционной системы. Такой интерфейс обычно реализуется с помощью набора соответствующих системных вызовов, которые принято называть системными вызовами безопасности.

Следует также иметь в виду, что сама операционная система может быть объектом атак злоумышленников. Основным методом противостояния таким атакам является использование специальной архитектуры операционной системы, подразумевающей локализацию всех базовых механизмов безопасности в рамках единой подсистемы, обладающей повышенной надежностью работы [6].

Совокупность средств, обеспечивающих информационную безопасность вычислительной системы, обычно объединяется в рамках комплекса средств защиты (КСЗ), включающего как модули ядра ОС, так и программы, работающие на уровне пользователя.

Основные функции КСЗ включают [4]:

- идентификацию и аутентификацию пользователя;
- дискреционное разграничение доступа к ресурсам;
- мандатное разграничение доступа к ресурсам;
- контроль повторного использования объектов;
- протоколирование событий;
- надежное восстановление;
- контроль состояния системы безопасности.

Далее рассмотрим различные аспекты перечисленных функций и особенности их реализации в рамках специализированной ОС Astra Linux [4].

Идентификация и аутентификация

Функция идентификации и аутентификации пользователей в ОС Astra Linux основывается на использовании механизма PAM (Pluggable Authentication Modules). Данный механизм представляет собой набор разделяемых библиотек, с помощью которых системный администратор может организовать процедуру аутентификации пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить произвольный сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования PAM.

Сценарии аутентификации описываются в конфигурационном файле /etc/pam.conf, а также в конфигурационных файлах, расположенных в каталоге /etc/pam.d/. Модули PAM располагаются в каталоге /lib/security в виде динамически загружаемых объектных файлов.

Предусмотрена возможность аутентификации как в рамках локального компьютера, так и в сети. В локальной системе аутентификация осуществляется с помощью локальной БД пользователей (/etc/passwd и т.д.).

При работе в сети аутентификация пользователей осуществляется централизованно по протоколу Kerberos [3], а в качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов LDAP (Lightweight Directory Access Protocol). Вся служебная информация пользователей может располагаться на выделенном сервере в распределенной гетерогенной сетевой среде. Сетевые сервисы, поддерживающие возможность аутентификации пользователей (web, FTP, почта), могут вместо локальных учетных записей использовать тот же каталог LDAP.

Благодаря предоставлению информации LDAP в иерархической древовидной форме разграничение доступа в рамках службы каталогов LDAP может быть основано на введении доменов. Сервисы LDAP позволяют разграничивать доступ пользователей к разным поддеревьям каталога, хотя по умолчанию в ОС реализуется схема одного домена.

Дискреционное разграничение доступа

В ОС Astra Linux реализован механизм дискреционного разделения доступа [4], ко-

торый заключается в том, что на защищаемые именованные объекты устанавливаются базовые права доступа в виде идентификаторов номинальных субъектов (UID и GID), которые вправе распоряжаться доступом к данному объекту, и прав доступа к объекту. Определяются три вида доступа: чтение (r), запись (w) и исполнение (x). Права доступа включают список из девяти пунктов: по три вида доступа для трех групп – пользователя-владельца, группы-владельца и всех остальных. Сопоставляя определенные виды доступа для каждой пары субъект–объект, можно описать полные правила разграничения доступа в рамках информационной системы.

При обращении процесса к объекту система проверяет совпадение идентификаторов владельцев процесса и владельцев файла и, в зависимости от результата, применяет ту или иную группу прав.

Права доступа файлового объекта могут быть изменены, если это разрешено текущими правилами.

Кроме общей схемы разграничения доступа, ОС поддерживает также списки ACL (Access Control List), с помощью которых можно для каждого объекта индивидуально задавать права доступа к нему всех субъектов.

Объектами доступа являются:

- файлы;
- соединения (сокеты);
- сетевые пакеты;
- механизмы IPC.

Механизм, реализующий дискреционное разграничение доступа, обеспечивает возможность санкционированного изменения списка пользователей и списка защищаемых файловых объектов.

Мандатное разграничение доступа

Механизм контроля мандатного разграничения доступа реализован, как и механизм дискреционного разграничения доступа, в ядре ОС Astra Linux4. При этом принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (r\w\x), мандатного контекста безопасности субъекта и мандатной метки объекта. Кроме того, при принятии решения могут учитываться полномочия субъекта.

Правила принятия решения могут быть записаны следующим образом. Пусть контекст безопасности субъекта содержит уровень L0 и категории C0, а мандатная метка объекта содержит уровень L1 и категории C1. Определим операции сравнения для уровней и категорий:

1) уровень L0 меньше уровня L1 (L0<L1), если численное значение L0 меньше численного значения L1;
2) уровень L0 равен уровню L1 (L0=L1), если численные значения L0 и L1 совпадают;
3) категории C0 меньше категорий C1 (C0<C1), если все биты набора C0 являются подмножеством набора бит C1;
4) категории C0 равны категориям C1 (C0=C1), если значения C0 и C1 совпадают;
5) операция записи разрешена, если L0=L1 и C0=C1;
6) операция чтения разрешена, если L0≥=L1 и C0≥C1;
7) операция исполнения разрешена, если L0≥L1 и C0≥C1.

В остальных случаях анализируются полномочия и тип мандатной метки. Тип метки может использоваться для того, чтобы изменять ее эффективное действие. Ненулевой тип метки может быть установлен только привилегированным процессом.

Механизм мандатного разграничения доступа затрагивает следующие подсистемы:

- механизмы IPC;
- стек TCP/IP (IPv4);
- файловые системы Ext2/Ext3/Ext4;
- сетевые файловые системы.

С каждым субъектом и объектом связаны: мандатный контекст безопасности и мандатная метка, соответственно.

При создании субъектом объект наследует метку на основе мандатного контекста безопасности процесса.

Контроль повторного использования объектов

Ядро ОС Astra Linux гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено правилами разграничения доступа (ПРД). Это означает, что средства IPC контролируются с помощью ПРД и процесс не может получить неочищенную память (как оперативную, так и дисковую).

В ОС реализован механизм, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа названного механизма снижает скорость выполнения операций удаления и усечения размера файла. Механизм является настраивае-

мым и позволяет обеспечить работу ФС ОС (Ext2/Ext3/Ext4) в одном из следующих режимов:

- данные любых удаляемых/урезаемых файлов в пределах заданной ФС предварительно очищаются маскирующей последовательностью;
- данные ФС освобождаются обычным образом (без предварительного маскирования).

Ядро ОС обеспечивает для каждого процесса в системе собственное изолированное адресное пространство на основе применения механизмов страничной организации памяти, а также трансляции виртуального адреса в физический. Одни и те же виртуальные адреса преобразуются в разные физические для разных адресных пространств процессов. Процесс не может несанкционированным образом получить доступ к адресному пространству другого процесса, т. к. он лишен возможности работать с физической памятью напрямую.

Механизм разделяемой памяти является санкционированным способом получить нескольким процессам доступ к одному и тому же участку памяти и находится под контролем дискреционных и мандатных ПРД.

Надежное восстановление

Основными причинами нарушения функционирования ОС являются сбои оборудования, приведшие к различным повреждениям файловой системы (ФС). К таковым относятся: сбои электропитания, повреждения носителей информации (жестких дисков), повреждения соединительных кабелей.

В процессе перезагрузки после сбоя автоматически выполняется программа проверки и восстановления ФС – fsck. Если повреждения ФС окажутся незначительными, то ее выполнения достаточно для обеспечения целостности ФС.

В случае обнаружения серьезных повреждений ФС данная программа может предложить перезагрузить компьютер в однопользовательский режим и произвести запуск программы fsck вручную. Администратор, контролирующий процесс загрузки ОС, после сбоя должен следовать инструкциям, выдаваемым программой fsck.

После завершения загрузки ОС следует проверить целостность файлов с помощью программы контроля целостности. Если в результате проверки найдутся поврежденные или измененные файлы, то следует восстановить поврежденные файлы с резервной копии.

Резервное копирование выполняется с целью получения копий данных, сохраняемых на случай их потери или разрушения. Подобные копии должны создаваться периодически, в соответствии с заранее установленным графиком.

Контроль целостности КСЗ

Для обеспечения контроля целостности (в т. ч. контроля целостности КСЗ) в ОС Astra Linux реализованы:

- средство подсчета контрольных сумм файлов и оптических дисков;
- средство контроля соответствия дистрибутиву;
- средства регламентного контроля целостности;
- средства создания замкнутой программной среды.

Для решения задач контроля целостности предназначена библиотека libgost, в которой для вычисления контрольных сумм реализована функция хэширования в соответствии с ГОСТ Р 34.11-20122. Названная библиотека используется в средствах подсчета контрольных сумм файлов и оптических дисков, контроля соответствия дистрибутиву и регламентного контроля целостности.

В ОС реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов. Проверка производится на основе контрольных сумм файлов.

Рассмотренные выше функции подсистемы безопасности ОС Astra Linux обеспечивают создание и функционирование защищенных информационных систем в соответствии с принятыми стандартами (см., например, приказ ФСТЭК от 18 февраля 2013 г. № 215). В рамках ОС поддерживаются все основные механизмы, предназначенные для реализации систем информационной безопасности. Данные механизмы имеют достаточно простой и интуитивно понятный интерфейс, обеспечивающий изучение их работы. Указанные обстоятельства позволяют рекомендовать к использованию ОС Astra Linux в качестве базовой системы в учебном процессе по направлению «Информационная безопасность».

Примечания

1. Безбогов, А. А. Методы и средства защиты компьютерной информации: учеб. пособие / А. А. Безбогов, А. В. Яковлев, В. Н. Шамкин. – Тамбов: Изд-во ТГТУ, 2006. – 120 с.

2. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2013. – 24 с.

3. Нестеров, С. А. Информационная безопасность и защита информации: учебное пособие. / С. А. Нестеров. СПб.: Изд-во политехн. ун-та, 2009. – 126 с.

4. Операционная система специального назначения «Astra Linux special edition». Руководство по КСЗ. в 2 ч. Ч. 1: 2012. – 100 с.

5. Приказ ФСТЭК от 18 февраля 2013 г. № 21. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных // Российская газета. – 2013. – 22 мая.

6. Таненбаум, Э. Современные операционные системы: монография / Э. Таненбаум. – СПб.: Питер, 2011. – 1116 с.

Окороков Валерий Анатольевич, канд. физ.-мат. наук, доцент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: okr@csu.ru

Valeriy Okorokov, kand. Sci. sciences, Associate Professor of Information Systems Security «South Ural State University». E-mail: okr@csu.ru

УДК 512.64 + 519.72 + 004.056.55

Медведева Н. В., Титов С. С.

ОПИСАНИЕ НЕЭНДОМОРФНЫХ СОВЕРШЕННЫХ ШИФРОВ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

В работе дано полное описание неэндоморфных совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров в случае, когда мощность алфавита шифрвеличин равна двум. Описание шифров приводится в терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Ключевые слова: *совершенные шифры, неэндоморфные шифры, максимальные шифры, дважды стохастические матрицы.*

Medvedeva N. V., Titov S. S.

THE DESCRIPTION OF NON-ENDOMORPHIC PERFECT CIPHERS WITH TWO PLAINTEXT VALUE

In this work it is given full description for non-endomorphic perfect ciphers which are absolutely immune against the attack on ciphertext, according to Shannon in a case when plaintext alphabet contains two elements (but ciphertext alphabet contains more than two elements). The description of these ciphers is provided in terms of linear algebra on the basis of Birkhoff's theorem of classification of doubly stochastic matrices. The set of possible values for aprioristic probabilities of elements in ciphertext alphabet of a perfect cipher is constructed.

Keywords: *perfect ciphers, non-endomorphic ciphers, maximum ciphers, doubly stochastic matrices.*

Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Пусть X, Y – конечные множества соответственно открытых текстов и шифрованных (закрытых) текстов, с которыми оперирует некоторый шифр замены, K – множество ключей, причем $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geq \lambda$. Под шифром будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах ℓ-грамм открытых текстов, шифрованных текстов и ключей [2, 3]. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются **совершенными**. Такие

шифры являются абсолютно стойкими к криптоатакам по шифртексту. В работе [1] полностью описаны **эндоморфные** ($|X|=|Y|$) совершенные шифры с минимально возможным числом ключей ($|K|=|Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершенные шифры с минимально возможным числом ключей исчерпываются шифрами гаммирования со случайной равновероятной гаммой.

Изучение **неэндоморфных** ($|X|<|Y|$) совершенных шифров в общем виде предполагает знание распределения вероятностей на множестве ℓ-грамм алфавита открытых текстов. В качестве стандартного аппарата исследования распределения вероятностей на ℓ-граммах используются дважды стохастические матрицы [4]. В работе [5] рассматривались комбинаторные проблемы современных аналогов совершенных шифров, в том числе неэндоморфных **неминимальных** ($|K|>|Y|$) совершенных шифров. Шифры, содержащие все инъекции из X в Y, т. е. для которых $|K|=\pi=\mu\cdot(\mu-1)\cdot\ldots\cdot(\mu-\lambda+1)$, называются **максимальными**. В работе [6] рассмотрены свойства неминимальных совершенных шифров. В частности, показано, что неминимальный совершенный шифр вкладывается в максимальный совершенный шифр.

Продолжая исследования [6], в данной работе в терминах линейной алгебры дано полное описание неэндоморфных максимальных совершенных по Шеннону шифров с мощностью алфавита шифрвеличин, равной двум. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность алфавита шифрвеличин равна двум. Пусть $X=\{x_1,x_2\}$ – алфавит открытых текстов; $Y=\{y_1,y_2,\ldots,y_\mu\}$ – алфавит шифрованных текстов, с которыми оперирует некоторый шифр замены; $K=\{k_1,k_2,\ldots,k_\pi\}$ – множество ключей. Здесь $|X|=\lambda=2, |Y|=\mu\geq 2, |K|=\pi=\mu\cdot(\mu-1)$.

Зашифрование открытого текста $x=x_{i_1}x_{i_2}\ldots x_{i_\ell}$, где $i_j\in\{1,2\}$, заключается в замене каждой шифрвеличины x_{i_j} на шифробозначение $y_{s_{i_j}}\in Y$, где $s_{i_j}\in\{1,2,\ldots,\mu\}$, в соответствии с одним из

$$|K|=A_{|Y|}^{|X|}=A_\mu^2=\frac{\mu!}{(\mu-2)!}=\mu\cdot(\mu-1)=\pi$$

всех инъективных отображений $e_k: X\to Y$, индексированных ключами $k\in K=\{k_1,k_2,\ldots,k_\pi\}$, занумерованными числами $1,2,\ldots,\pi$. Инъективное отображение e_k, $k\in K$, при котором

$$e_k(x_1)=y_s=s \text{ и } e_k(x_2)=y_t=t,$$

будем также обозначать e_{st}, где $s,t=1,2,\ldots,\mu$.

Пусть P_{st} – вероятность того, что при зашифровании шифрвеличин X_1 и X_2 будет выбрано инъективное отображение e_{st}, т. е.

$$P_{st}=P\{e_{st}(x_1)=s \,\&\, e_{st}(x_2)=t\},$$

где $y_s\neq y_t$. Если $s=t$, то, в силу инъективности, $P_{st}=0$.

Обозначим через $P=\|P_{st}\|_{s,t=1}^{\mu}$ – квадратную матрицу порядка μ такую, что

$$\forall s:\sum_{t=1}^{\mu}P_{st}=p_s,\quad \forall t:\sum_{s=1}^{\mu}P_{st}=p_t,\quad p_1+p_2+\ldots+p_\mu=1. \tag{1}$$

Требуется описать множество возможных значений априорных вероятностей шифробозначений $p_s=P\{y=y_s\}=P\{y=s\}$, $s=1,2,\ldots,\mu$ и найти общий вид матрицы P, удовлетворяющей условию (1) совершенности шифра, в зависимости от значений вероятностей P_s.

В частности, в примере 2.2.10 из [3] $X=\{x_1,x_2\}$, $Y=\{y_1,y_2,y_3\}$, $k\in K=\{1,2,\ldots,6\}$, т. е. при $\lambda=2$, $\mu=3$, $\pi=6$, таблица зашифрования имеет вид

$K\backslash X$	x_1	x_2	$P_{st}=P\{e_{st}(x_1)=s \,\&\, e_{st}(x_2)=t\},$
k_1	1	2	$P_{12}=P\{k=k_1\}=19/80$
k_2	1	3	$P_{13}=P\{k=k_2\}=3/20$
k_3	2	1	$P_{21}=P\{k=k_3\}=21/80$
k_4	2	3	$P_{23}=P\{k=k_4\}=1/10$
k_5	3	1	$P_{31}=P\{k=k_5\}=1/8$
k_6	3	2	$P_{32}=P\{k=k_6\}=1/8$

Здесь априорные вероятности шифробозначений $p_s = P\{y = y_s\} = P\{y = s\}$, где s=1,2,3, равны:

$$p_1 = P\{y = 1\} = P\{k = k_1 \,\&\, x = x_1\} + P\{k = k_2 \,\&\, x = x_1\} + P\{k = k_3 \,\&\, x = x_2\} +$$
$$+ P\{k = k_5 \,\&\, x = x_2\} = \left(\frac{19}{80} + \frac{3}{20}\right)P\{x = x_1\} + \left(\frac{21}{80} + \frac{1}{8}\right)P\{x = x_2\} =$$
$$= \frac{31}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{31}{80};$$

$$p_2 = P\{y = 2\} = P\{k = k_3 \,\&\, x = x_1\} + P\{k = k_4 \,\&\, x = x_1\} + P\{k = k_1 \,\&\, x = x_2\} +$$
$$+ P\{k = k_6 \,\&\, x = x_2\} = \left(\frac{21}{80} + \frac{1}{10}\right)P\{x = x_1\} + \left(\frac{19}{80} + \frac{1}{8}\right)P\{x = x_2\} =$$
$$= \frac{29}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{29}{80};$$

$$p_3 = P\{y = 3\} = P\{k = k_5 \,\&\, x = x_1\} + P\{k = k_6 \,\&\, x = x_1\} + P\{k = k_2 \,\&\, x = x_2\} +$$
$$+ P\{k = k_4 \,\&\, x = x_2\} = \left(\frac{1}{8} + \frac{1}{8}\right)P\{x = x_1\} + \left(\frac{3}{20} + \frac{1}{10}\right)P\{x = x_2\} =$$
$$= \frac{20}{80}(P\{x = x_1\} + P\{x = x_2\}) = \frac{20}{80}.$$

Проверим, что $p_1 + p_2 + p_3 = \frac{31}{80} + \frac{29}{80} + \frac{20}{80} = 1.$

Апостериорные вероятности шифробозначений y_s, s=1,2,3 соответственно равны:

$$P\{y = 1 \mid x = x_1\} = P\{y = 1 \mid k = k_1\} + P\{y = 1 \mid k = k_2\} = \frac{19}{80} + \frac{3}{20} = \frac{31}{80};$$

$$P\{y = 1 \mid x = x_2\} = P\{y = 1 \mid k = k_3\} + P\{y = 1 \mid k = k_5\} = \frac{21}{80} + \frac{1}{8} = \frac{31}{80};$$

$$P\{y = 2 \mid x = x_1\} = P\{y = 2 \mid k = k_3\} + P\{y = 2 \mid k = k_4\} = \frac{21}{80} + \frac{1}{10} = \frac{29}{80};$$

$$P\{y = 2 \mid x = x_2\} = P\{y = 2 \mid k = k_1\} + P\{y = 2 \mid k = k_6\} = \frac{19}{80} + \frac{1}{8} = \frac{29}{80};$$

$$P\{y = 3 \mid x = x_1\} = P\{y = 3 \mid k = k_5\} + P\{y = 3 \mid k = k_6\} = \frac{1}{8} + \frac{1}{8} = \frac{20}{80};$$

$$P\{y = 3 \mid x = x_2\} = P\{y = 3 \mid k = k_2\} + P\{y = 3 \mid k = k_4\} = \frac{3}{20} + \frac{1}{10} = \frac{20}{80}.$$

При этом для вероятностей $P_{st} = P\{e_{st}(x_1) = s \,\&\, e_{st}(x_2) = t\}$, s=1,2,3, выполняются равенства:

$$P\{y = 1 \mid x = x_1\} = P_{12} + P_{13} = \frac{31}{80};\ P\{y = 1 \mid x = x_2\} = P_{21} + P_{31} = \frac{31}{80};$$

$$P\{y = 2 \mid x = x_1\} = P_{21} + P_{23} = \frac{29}{80};\ P\{y = 2 \mid x = x_2\} = P_{12} + P_{32} = \frac{29}{80};$$

$$P\{y = 3 \mid x = x_1\} = P_{31} + P_{32} = \frac{20}{80};\ P\{y = 3 \mid x = x_2\} = P_{13} + P_{23} = \frac{20}{80}.$$

Следовательно, для каждого шифробозначения y_s, $s=1,2,3$ априорные вероятности совпадают с апостериорными. Это, согласно [3], эквивалентно равенству априорных и апостериорных вероятностей шифрвеличин, т. е. матрица

$$P = \| P_{st} \|_{s,t=1}^{3} = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} = \begin{pmatrix} 0 & \frac{19}{80} & \frac{3}{20} \\ \frac{21}{80} & 0 & \frac{1}{10} \\ \frac{1}{8} & \frac{1}{8} & 0 \end{pmatrix}$$

удовлетворяет условию (1) совершенности шифра.

В работе [6] показано, что искомое распределение вероятностей на множествах ℓ-грамм шифрованных текстов и ключей, при котором максимальный неэндоморфный шифр будет совершенным, представляет собой некоторое выпуклое тело P^{ℓ} – многогранник в многомерном евклидовом пространстве.

В случае, когда мощность алфавита шифрвеличин равна двум, многогранник P^{ℓ} допускает полное описание на основе теоремы Биркгофа о классификации дважды стохастических матриц. В этом описании существенно используется тот факт, что матрица P с неотрицательными элементами, удовлетворяющая условию (1), есть линейная комбинация с неотрицательными коэффициентами δ_Z дважды стохастических главных подматриц T_Z, где Z – непустое множество номеров строк и столбцов, а именно

$$P = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \delta_Z T_Z.$$

Сумма всех элементов каждой матрицы T_Z равна $|Z|$. Для каждого $Z \subset \{1,2,\ldots,\mu\}$, $Z \neq \varnothing$ матрица P_Z равновероятных распределений определяется по формуле

$$P_Z = \frac{1}{|Z|} \cdot T_Z.$$

Сумма всех элементов каждой матрицы P_Z равна единице, как и для матрицы P. Следовательно,

$$1 = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \delta_Z \cdot |Z| = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \rho_Z,$$

где $\rho_Z = |Z| \cdot \delta_Z$ и $\rho_Z \geq 0$, т. е. для матрицы P выполняются условия

$$P = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \rho_Z P_Z, \quad \sum_{\substack{Z \subset \{1,2,\ldots,\mu\} \\ Z \neq \varnothing}} \rho_Z = 1. \tag{2}$$

Теорема 1. Матрица P с неотрицательными элементами, удовлетворяющая условию (1), лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений и определяется формулой (2).

Рассмотрим примеры, иллюстрирующие теорему 1.

Пример 1. Пусть $\mu = 2$ и матрица P имеет нулевую диагональ. Тогда $p_{12} = p_{21} = p_1 = p_2 = \frac{1}{2}$ и матрица P единственна:

$$P = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{2} \cdot T,$$

где T – дважды стохастическая матрица. Это частный случай теоремы Шеннона для эндоморфного минимального шифра.

Пример 2. Пусть $\mu = 3$, матрица P имеет нулевую диагональ и

$$a = \tau_1 \cdot \rho_{\{1,2,3\}} \geq 0,\ b = \tau_2 \cdot \rho_{\{1,2,3\}} \geq 0,$$

$$c = \rho_{\{1,2\}} \geq 0,\ d = \rho_{\{1,3\}} \geq 0,\ e = \rho_{\{2,3\}} \geq 0$$

где произвольные параметры τ_1, τ_2, ρ_Z таковы, что

$$\tau_1 \geq 0, \tau_2 \geq 0, \tau_1 + \tau_2 = 1, \rho_Z \geq 0,$$

$$\rho_{\{1,2,3\}} + \rho_{\{1,2\}} + \rho_{\{1,3\}} + \rho_{\{2,3\}} = a + b + c + d + e = 1$$

Тогда при $\lambda = 2$ и $\mu = 3$ матрица P в общем случае определяется формулой

$$P = \frac{1}{3}a\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{3}b\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \frac{1}{2}c\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} +$$

$$+\frac{1}{2}d\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{2}e\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{3}a + \frac{1}{2}c & \frac{1}{3}b + \frac{1}{2}d \\ \frac{1}{3}b + \frac{1}{2}c & 0 & \frac{1}{3}a + \frac{1}{2}e \\ \frac{1}{3}a + \frac{1}{2}d & \frac{1}{3}b + \frac{1}{2}e & 0 \end{pmatrix}$$

где $a, b, c, d, e \geq 0$ – произвольные параметры такие, что $a + b + c + d + e = 1$.

Отметим, что для любых $a, e \geq 0$, где $2a + 3e = \frac{3}{5}$, и однозначно по ним определенным параметрам $b = a + \frac{3}{40}$, $c = e + \frac{11}{40}$, $d = e + \frac{1}{20}$, получаются числовые значения примера 2.2.10 из [3]. В частности, они получаются при крайних значениях параметров: $a = 0, e = \frac{1}{5}$ и $a = \frac{3}{10}, e = 0$.

Теорема 2. Набор чисел $p_1, \ldots, p_\mu$ при $\mu \geq 2$ может быть набором априорных вероятностей шифрвеличин совершенного шифра в модели $\Sigma_в$ с мощностью алфавита шифрвеличин, равной двум, тогда и только тогда, когда эти числа удовлетворяют условиям

$$p_1 + \ldots + p_\mu = 1,\ 0 \leq p_i \leq \frac{1}{2},\ i = 1, 2, \ldots, \mu. \qquad (3)$$

В приложении к совершенным шифрам это означает, что любой набор чисел $p_i, i = 1, 2, \ldots, \mu$ с условиями (3) может быть набором априорных вероятностей шифробозначений совершенного шифра.

Таким образом, в работе полностью описаны неэндоморфные совершенные шифры в случае, когда мощность алфавита шифрвеличин равна двум.

Примечания

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Наука, 1963. – С. 333–402.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

3. Зубов А. Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003. – 160 с.

4. Birkhoff G. D. Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman, 1946. – Ser. A. – V. 5. – С. 147–151.

5. Титов С. С., Гутарин Д. С., Коновалова С. С., Титов Е. С., Тимин В. И. Комбинаторные проблемы существования совершенных шифров // Труды ИММ УрО РАН. – 2008. – Т. 13. – № 4. – С. 61–73.

6. Медведева Н. В., Титов С. С. О неминимальных совершенных шифрах // Прикладная математика. Приложение. – 2013. – № 6. – С. 42–44.

Медведева Наталья Валерьевна, к. ф.-м. н., доцент, доцент кафедры «Высшая и прикладная математика» УрГУПС, г. Екатеринбург. E-mail: medvedeva_n_v@mail.ru.

Титов Сергей Сергеевич, д. ф.-м. н., профессор, профессор кафедры «Высшая и прикладная математика» УрГУПС, Екатеринбург. E-mail: stitov@usaaa.ru.

Natalia Valerievna Medvedeva, PhD Physics and Mathematics, associate professor of Ural State University of Railway Transport. E-mail: medvedeva_n_v@mail.ru.

Sergey Sergeevich Titov, DSc Physics and Mathematics, Professor of Ural State University of Railway Transport. E-mail: stitov@usaaa.ru.

УДК 004.738 : 519.23 + 519.237.8

Попов Е. Ф., Тюкова А. А., Фучко М. М., Захаров А. А.

ВЫЯВЛЕНИЕ НЕТИПИЧНЫХ СОБЫТИЙ СРЕДСТВАМИ СТАТИСТИЧЕСКОГО АНАЛИЗА

В работе изучается вопрос о применимости алгоритмов статистического анализа для выявления нетипичных событий и состояний в различных информационных системах. Рассматривается возможность применения кластерного анализа для выявления нетипичных потоков трафика в сети передачи данных, а также его эффективность при различной интерпретации характеристик потоков сетевого трафика.

Ключевые слова: *статистический анализ, кластерный анализ, сети передачи данных, выявление аномалий, система обнаружения вторжений.*

Popov E. F., Tyukova A. A. Fuchko M. M., Zakharov A. A.

IDENTIFICATION ATYPICAL EVENTS BY MEANS STATISTICAL ANALYSIS

We study the question of the applicability of the statistical analysis to detect unusual events and conditions in various information systems. The possibility of using cluster analysis to identify unusual traffic flows in a data network, as well as its efficacy in the different interpretations of network traffic flow characteristics.

Keywords: *statistical analysis, cluster analysis, data network, anomaly detection, intrusion detection system.*

Введение

В условиях быстрого развития информационных технологий постоянно разрабатываются новые методы атак на информационные системы, что требует непрерывного совершенствования средств защиты информации. Так как предусмотреть все способы атак на информационную систему зачастую не представляется возможным, оптимальным решением является выявление нетипичных событий и состояний системы.

Для выявления отклонений необходимы показатели, которые отображают типичное состояние информационной системы и могут выступать в качестве эталона для сопоставления с данными, обрабатываемыми в реальном времени. Применение алгоритмов статистического анализа к данным, собранным в период штатного функционирования, позволяет выделить статистические показатели, при сравнении с которыми можно выявить нетипичные события и состояния, являющиеся потенциально опасными для информационной системы.

В данной работе изучается вопрос о применимости алгоритмов статистического анализа для выявления нетипичных событий и состояний на примере потоков трафика в се-

тях передачи данных. Рассматривается эффективность применения результатов кластерного анализа в реальном времени при различной интерпретации характеристик потоков сетевого трафика. По результатам применения кластерного анализа к потокам трафика в сети передачи данных оценивается возможность применения используемого метода для выявления нетипичных событий и состояний в различных подсистемах и элементах информационной инфраструктуры.

Сбор и интерпретация статистических данных

Сложность применения статистического анализа в данном контексте заключается в том, что применяемые алгоритмы должны быть адаптированы для обработки данных в реальном времени и должны производить интеллектуальный анализ, учитывающий не только текущее состояние системы или состояния за короткий промежуток времени. Наиболее ценными являются данные, собранные за длительные периоды штатного функционирования, которые являются необходимыми для наиболее точного выявления типичных событий и состояний системы [1].

Для обработки характеристик, собранных за длительный период, важно применять алгоритмы статистического анализа, не только адаптированные для обработки большого количества данных, но и способные учитывать степень устаревания, что является необходимым для адаптации к изменениям в информационной системе. Наиболее оптимальными являются алгоритмы, которые способны производить анализ не только на базе набора статистических данных, но и с учетом предыдущих результатов работы алгоритмов статистического анализа.

События и состояния могут рассматриваться как объекты, обладающие рядом характеристик. Полученные объекты могут быть использованы в качестве статистических единиц для таких алгоритмов статистического анализа, как алгоритмы кластеризации. Рассмотрим применение статистического анализа для выявления нетипичных состояний на примере.

Наиболее удобным для рассмотрения является пример применения статистического анализа к потокам трафика в сети передачи данных. Для сбора информации о потоках трафика могут использоваться сенсоры, базирующиеся на протоколе NetFlow. Подобные сенсоры позволяют получить следующие характеристики:

- IP-адреса отправителя и назначения;
- протоколы сетевого и транспортного уровня;
- номера портов (TCP/UDP), позволяющие определить используемый протокол прикладного уровня;
- время;
- объем переданных данных;
- средний размер пакетов данных [2].

Полученные характеристики необходимо адаптировать для применения кластерного анализа.

IP-адрес не может применяться для кластерного анализа в чистом виде, так как не характеризует никаких особенностей потока трафика, и данные, передаваемые на различные адреса, могут быть предназначены для работы с одним и тем же сервисом. Например, таким как поисковик Google, который обеспечивает балансировку нагрузки за счет соответствия своему основному доменному имени ряда различных IP-адресов, что не всегда возможно отслеживать автоматически в процессе кластерного анализа [3].

Но за счет адреса назначения можно выявить ряд особенностей потока трафика, например, выявить для внутренней или для внешней сети предназначен поток трафика, что является важной характеристикой в процессе анализа. Также, опираясь на адрес отправителя, можно выявить, какие устройства или какая группа пользователей располагаются в данной подсети, определив, из какой подсети инициирован поток трафика.

Протокол прикладного уровня, который определяется номерами портов, является одной из ключевых характеристик, которая может быть интерпретирована различным образом. Можно разделять статистические единицы на множество классов, считая потоки данных каждого из протоколов прикладного уровня отдельными классами. Также протоколы прикладного уровня могут быть разделены на классы по их функциональному предназначению:

- получение информации с веб-сайтов;
- передача файлов;
- мгновенный обмен сообщениями;
- потоковая передача данных;
- удаленное управление;
- и т. д.

При сравнении потоков сетевого трафика, относящихся к различным классам, было

выявлено, что остальные характеристики, такие как объем передаваемых данных, длительность передачи данных, средний размер пакета, зависит от класса потока трафика, определенного по функциональному предназначению протокола прикладного уровня. И характеристики потоков сетевого трафика различных протоколов прикладного уровня, относящихся к одному классу, имеют сходство намного большее, чем в случае с протоколами, относящимися к разным классам [4].

Применение статистического анализа

Необходимо выделить единицу потока трафика, к которой будет применяться статистический анализ. В данном контексте статистической единицей могут являться:

- поток трафика от уникального отправителя уникальному получателю за весь период передачи данных (период активности сессии);
- поток трафика от уникального отправителя уникальному получателю за заданный промежуток времени.

Анализ потока за полный период передачи данных между двумя узлами представляет наиболее точную характеристику природы трафика и является наиболее ценным для статистического анализа. Но статистика, составленная на базе информации о сетевом трафике, переданном за полный период активности сессии, может быть использована для обнаружения нетипичных потоков данных только после завершения сессии, что значительно увеличивает время реакции системы.

При использовании в качестве статистических единиц сегментов, выделенных из общего потока, ограниченных небольшими промежутками времени, например интервалами в 30 секунд, снижается точность статистического анализа, но появляется возможность использования результата статистического анализа для обнаружения нетипичных действий в реальном времени с максимальным временем реакции, равным выбранному интервалу времени для статистической единицы [5].

Каждую отдельную статистическую единицу можно представить в виде точки, расположенной в многомерном пространстве, каждое из измерений которого представляет собой одну из характеристик потока трафика. Применение алгоритма кластеризации позволит выявить области с высокой концентрацией точек и объединить их в кластеры. В результате работы алгоритмов будут получены кластеры, отображающие наборы характеристик, свойственные потокам сетевого трафика, передаваемого при штатном функционировании системы [6].

На базе результатов вычислений могут быть выделены правила, описывающие значения ряда характеристик, свойственные для полученных кластеров, которые могут стать эталонными для определения типичности потоков трафика. Наличие правил, описывающих типичные потоки трафика, открывает возможность производить в реальном времени контроль, лежат ли значения характеристик текущих потоков трафика в рамках типичных для данной информационной системы.

Выводы

В результате исследования было выявлено, что интерпретация статистических единиц как объектов, обладающих рядом характеристик, позволяет адаптировать статистические данные о событиях и состояниях различных подсистем для анализа с применением алгоритмов кластеризации. Необходимым и достаточным для применения кластерного анализа является наличие исчисляемых характеристик событий или состояний. На эффективность алгоритмов кластеризации влияет равномерность распределения и зависимость характеристик статистических единиц.

Было определено, что по результатам кластерного анализа может быть разработан ряд правил, определяющий типичные значения характеристик статистической единицы, которые могут быть применены для выявления нетипичных событий или состояний в реальном времени без необходимости повторного применения алгоритмов статистического анализа.

На примере применения кластерного анализа для выявления нетипичных потоков трафика в сети передачи данных обнаружена зависимость эффективности алгоритмов кластеризации от интерпретации характеристик статистических единиц. Определено, что классификация статистических единиц по характеристикам, не имеющим числового значения, может оказывать высокое влияние на эффективность кластерного анализа при условии зависимости от них значений исчисляемых характеристик.

Примечания

1. Babenko G. V., Belov S. V. Identification of network abnormalities using methods of statistical analysis //European researcher – 2011. – T. 1. – No. 5.

2. Claise D. Cisco Systems NetFlow Services Export Version 9 // IETF RFC 3954 URL: http://www.ietf.org/rfc/rfc3954 (датаобращения 08.12.2014)

3. Barroso L. A., Dean J., Holzle U. Web search for a planet: The Google cluster architecture //Micro, Ieee. – 2003. – T. 23. – No. 2. – P. 22–28.

4. Soysal M., Schmidt E. G. Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison //Performance Evaluation. – 2010. – T. 67. – No. 6. – P. 451–467.

5. Костенко С. А. Технология применения многомерного шкалирования и кластерного анализа // Фундаментальные исследования. – 2012. – №. 11. – С. 927–930.

6. Дюран Б., Оделл П. Кластерный анализ //М.: Статистика. – 1977. – Т. 15.

Попов Евгений Фёдорович, аспирант ТюмГУ. E-mail: efpopov@gmail.com

Тюкова Александра Александровна, аспирант ТюмГУ. E-mail: tyukovaaa@kbinform.ru

Фучко Михаил Михайлович, аспирант ТюмГУ. E-mail: mikhalich@russia.ru

Захаров Александр Анатольевич, д. т. н., профессор ТюмГУ

Popov Evgeniy, a graduate student Tyumen State University. E-mail: efpopov @ gmail.com

Tyukova Aleksandra, a graduate student Tyumen State University. E-mail: tyukovaaa@kbinform.ru

Fuchko Mihail, Tyumen State University, graduate student. E-mail: mikhalich@russia.ru

Zakharov Alexander, Ph.D., professor of Tyumen State University

УДК 003.26 + 004.056.5

Зюляркина Н. Д.

ЭЛЕМЕНТЫ БОЛЬШИХ ПОРЯДКОВ В ЛИНЕЙНЫХ ГРУППАХ И МОДИФИКАЦИЯ СИСТЕМЫ ЭЛЬ-ГАМАЛЯ

Большое распространение в настоящее время получили криптосистемы, основанные на задаче нахождения дискретного логарифма. В данной работе описывается криптосистема с открытым ключом, являющаяся модификацией системы Эль-Гамаля. Схема Эль-Гамаля — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле, включающая в себя алгоритм шифрования и алгоритм цифровой подписи. А также рассматривается зарубежное и российское законодательство в сфере криптографии. Проанализированы подходы к обучению студентов по данному направлению.

Ключевые слова: *криптосистема с открытым ключом, группа, порождающий элемент.*

Zyulyarkina N. D.

ELEMENTS MORE ORDER LINEAR GROUPS, AND MODIFICATION OF THE ELGAMAL

Widespread currently received cryptosystems based on the problem of finding the discrete logarithm. This paper describes a public key cryptosystem, which is a modification of the El-Gamal. Driving El-Gamal - a public key cryptosystem based on the difficulty of calculating discrete logarithms in a finite field that includes an encryption algorithm and digital signature algorithm. Also considered foreign and Russian legislation in the field of cryptography. Approaches to teaching students in this area.

Keywords: *public-key cryptosystem, the group generating element.*

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» У. Диффи и М. Хеллмана, опубликованной в 1976 году [1].

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования, при которой открытый ключ передается по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах и стандартах цифровой подписи.

Для построения криптосистемы с открытым ключом выбирается класс задач, для которого в произвольном случае не известен

эффективный алгоритм решения и в этом классе выделяется подзадача, для которой такой алгоритм существует. Выбранную задачу маскируют под задачу общего вида и на основе ее выбирают ключ шифрования. В качестве секретного ключа используется информация, позволяющая перевести выбранную задачу в исходный вид.

Большое распространение в настоящее время получили криптосистемы, основанные на задаче нахождения дискретного логарифма. К ним можно отнести схему распределения ключей Диффи – Хеллмана, схему Эль-Гамаля, цифровую подпись Шнорра и т. д. Классическое описание этих систем предполагает использование мультипликативных групп конечных полей простого порядка. Но развитие технических средств сделало системы, использующие традиционные ключи, более уязвимыми. В связи с этим особенно активно изучаются способы, основанные на вычислениях в специально подобранных группах. Отметим в качестве примера группы точек эллиптических кривых, которые используются в обобщенной схеме Эль-Гамаля, применяемой в стандартах цифровой подписи. К достоинствам этих групп следует отнести наличие элементов большого порядка и сложность нахождения дискретного логарифма.

Задача нахождения дискретного логарифма и элементы больших порядков

Пусть G – циклическая группа порядка n, порожденная элементом g, а x – элемент из G. Назовем элемент m из Z_n *логарифмом x по основанию g*, если выполняется равенство $g^m=x$. Если G имеет бесконечный порядок, то m выбирается из множества целых чисел.

Задачей дискретного логарифмирования назовем нахождение m по известным g и x. Сложность этой задачи связана с видом группы G. Если в качестве G взять множество целых чисел с операцией сложения, а элемент g выбрать равным 1, то, очевидно, указанная задача будет решаться тривиально, так как $m=x$. Но ситуация кардинально меняется, если в качестве G взять специальным образом выбранную матричную группу.

Пример 1. Рассмотрим общую линейную группу $GL_n(R)$ и выберем в ней элемент $g=\begin{pmatrix}-14 & -9\\ 25 & 16\end{pmatrix}$. Пусть $G=\langle g\rangle$. Можно показать, что g имеет бесконечный порядок и, следовательно, G изоморфна группе целых чисел. Но задача нахождения дискретного логарифма в этой группе уже далеко не так проста, как для Z. Ведь уже далеко не очевидно, что решением уравнения $g^m=\begin{pmatrix}-224 & -135\\ 375 & 226\end{pmatrix}$ будет $m=15$.

Для того чтобы задача о нахождении дискретного логарифма была трудноразрешимой, нужно подобрать подходящую группу, а в ней подходящий элемент. Необходимым условием подбора элемента является большое значение его порядка, так как для элементов малых порядков дискретный логарифм можно найти с помощью перебора. Но это условие не является достаточным, что следует из примера $G=Z$. Группами, в которых есть элементы с указанными свойствами, являются мультипликативные группы конечных полей, группы точек эллиптических кривых и линейные (матричные) группы. Отметим, что решение задачи нахождения дискретного логарифма для мультипликативных групп конечных полей можно найти с помощью метода «Шаг младенца – шаг великана» и метода исчисления порядка, которые более эффективны, чем метод перебора. Метод «Шаг младенца – шаг великана» является универсальным и применим к любой конечной циклической группе. Но при большом значении порядка группы он не дает существенного выигрыша во времени по сравнению с методом перебора. Метод исчисления порядка является более быстрым, но он специфичен и не переносится на случай матричных групп.

Модификация криптосистемы Эль-Гамаля с использованием линейных групп

Схема Эль-Гамаля — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле, включающая в себя алгоритм шифрования и алгоритм цифровой подписи. Она лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94). Опишем классический вариант данной схемы.

Генерация ключей.

1. Генерируется случайное простое число p.
2. Выбирается случайный примитивный элемент x поля Z_p.
3. Выбирается случайное целое число a такое, что $2 \le a \le p-2$.

4. Вычисляется x^a.

Открытым ключом является тройка (p, x, x^a), а секретным ключом — число a .

Алгоритм шифрования.

1. Исходный текст представляется в виде последовательности элементов из Z_p.
2. Каждый элемент m открытого текста шифруется следующим образом:

a) Выбирается сессионный ключ r — случайное целое число, такое, что $1 < r < p - 1$;

b) Вычисляются числа x^r и $m(x^a)^r$.

Пара чисел $(x^r, m(x^a)^r)$ является шифр-текстом, соответствующим m.

Алгоритм расшифровки.

1. Шифр-текст разбивается на пары (c, b).
2. По каждой паре восстанавливается элемент открытого текста по формуле $m = (c^a)^{-1} b$.

Теперь дадим описание модификации данной схемы, использующей линейные группы.

Генерация ключей.

1. Выбирается линейная группа $G=GL_n(K)$, где K – некоторое коммутативное кольцо с единицей (например, кольцо вычетов).
2. Выбирается случайный элемент x группы G большого порядка p.
3. Выбирается случайное целое число a такое, что $2 \le a \le p-1$.
4. Вычисляется x^a.

Открытым ключом является тройка (G, x, x^a), а секретным ключом — число a.

Алгоритм шифрования.

1. Исходный текст представляется в виде последовательности элементов из $M_n(K)$.
2. Каждый элемент m открытого текста шифруется следующим образом:

a) Выбирается сессионный ключ r — случайное целое число, такое, что $1 < r < p$;

b) Вычисляются элементы x^r и $m(x^a)^r$.

Пара чисел $(x^r, m(x^a)^r)$ является шифр-текстом, соответствующим m.

Алгоритм расшифровки.

1. Шифр-текст разбивается на пары (c, b).
2. По каждой паре восстанавливается элемент открытого текста по формуле $m=b(c^a)^{-1}$.

Пример 2. Пусть открытым ключом в описанной модификации является набор $(GL_2(137), \begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}, \begin{pmatrix} 124 & 95 \\ 96 & 15 \end{pmatrix})$, а секретный ключ $a=41$. Зашифруем сообщение $m=\begin{pmatrix} 2 & 5 \\ 8 & 9 \end{pmatrix}$:

a) Выберем сеансовый ключ $r=83$;

b) Вычислим $x^r=\begin{pmatrix} 113 & 62 \\ 54 & 26 \end{pmatrix}$ и $m(x^a)^r=\begin{pmatrix} 117 & 76 \\ 89 & 115 \end{pmatrix}$

Зашифрованный текст представим матрицей $\begin{pmatrix} 113 & 62 & 117 & 76 \\ 54 & 26 & 89 & 115 \end{pmatrix}$.

Для расшифровки данного сообщения выполним следующие действия:

a) Разобьем полученное сообщение на две матрицы $b=\begin{pmatrix} 113 & 62 \\ 54 & 26 \end{pmatrix}$ и $c=\begin{pmatrix} 117 & 76 \\ 89 & 115 \end{pmatrix}$

b) Используя секретный ключ $a=83$, найдем исходное сообщение по формуле $m=bc^{-83}$.

В данном примере элемент $\begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}$ имеет в группе $GL_2(137)$ порядок, равный 136.

Элементы больших порядков в линейных группах

Для выбора ключа в описанной модификации нужно иметь в своем распоряжении матрицу достаточно большого порядка. Поэтому особую важность представляет информация о порядках элементов в линейных группах и способах построения элементов заданного порядка. Если рассматривается группа $GL_n(Z_m)$, то с помощью китайской теоремы об остатках ситуацию можно свести к рассмотрению групп $GL_n(Z_q)$, где q является примарным числом. Для усложнения задачи дискретного логарифмирования можно преобразовывать элемент x с помощью сопряжения.

Пример 3. Элемент $x=\begin{pmatrix} 4 & 9 \\ 136 & 135 \end{pmatrix}$ в группе $GL_2(137)$ из предыдущего примера был получен как $y^h=h^{-1}yh$, где $h=\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, $y=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Элемент y имеет порядок 136 и задача дискретного логарифмирования для него эквивалентна задаче нахождения дискретного логарифма в поле порядка 137. Легко заметить, что задача дискретного логарифмирования для элемента x является более сложной.

Примечания

1. Diffie W, Hellman M. E. New Directions in Cryptography. // IEEE Transactions on Information Theory. V. TI-22,1977, pp 644–654.

2. Саломаа А. Криптография с открытым ключом = Public-Key Cryptography. — Springer-Verlag, 1990. — С. 102–150.

Зюляркина Наталья Дмитриевна, кандидат физ.-мат. наук, доцент, преподаватель кафедры «Безопасность информационных систем», г. Челябинск. E-mail: toddeath@yandex.ru

Zyulyarkina Natalia, Candidate of Physics and Mathematics. , Associate Professor, Lecturer, Department of Information Systems Security, Chelyabinsk. E-mail: toddeath@yandex.ru

УДК 056 + 002 : 004.056 + 378.016 : 002 : 004.056

Филиппов А. С., Астахова Л. В.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТ ИЗУЧЕНИЯ В ВУЗЕ

В данной статье обоснован процесс управления инцидентами информационной безопасности на основе российских и зарубежных стандартов как объект изучения будущими специалистами по защите информации в высшем учебном заведении. В процессе подготовки специалистов по защите информации в вузе важную роль играет освоение процессов управления инцидентами информационной безопасности на основе российских и зарубежных стандартов. Рассмотрены различные национальные стандарты в области информационных технологий и информационной безопасности, а также освещены международные стандарты. Кроме основ законодательства Российской Федерации, государственных стандартов в области информационных технологий (как отечественных, так зарубежных), студентов вуза необходимо обучать судебной практике в области расследования инцидентов информационной безопасности, а также программным продуктам для получения доказательной базы и документированию процесса управления инцидентами в целом. Благодаря этим знаниям и умениям обучающиеся смогут самостоятельно строить алгоритмы управления инцидентами информационной безопасности в организации.

Ключевые слова: *инциденты, информационная безопасность.*

Filippov A. S., Astakhova L. V.

INCIDENT MANAGEMENT INFORMATION SAFETY AS AN OBJECT OF STUDY IN HIGH SCHOOL

In this paper based process management of information security incidents based on Russian and foreign standards as an object of study of the future of information security experts in higher education. During the preparation of information security specialists at the university plays an important role the development of management processes of information security in-

cidents based on Russian and foreign standards. Different national standards in the field of information technology and information security. And also covered international standards. In addition to the basics of the Russian legislation, state standards in the field of information technologies (both domestic foreign) university students should be taught jurisprudence in the investigation of incidents of information security, as well as software products to provide evidence and documentation of the incident management process as a whole. With this knowledge and skills students will be able to build their own control algorithms for information security incidents within the organization.

Keywords: *accidents, information security.*

В процессе подготовки специалистов по защите информации в вузе важную роль играет освоение процессов управления инцидентами информационной безопасности на основе российских и зарубежных стандартов.

Для управления инцидентами информационной безопасности нужны специальные знания: основ законодательства Российской Федерации, а также международных и национальных стандартов.

В российском законодательстве используются различные национальные стандарты в области информационных технологий и информационной безопасности, например ГОСТ Р ИСО/МЭК 18044-2007 [1]. Стандарт описывает инфраструктуру управления инцидентами информационной безопасности в рамках циклической модели PDCA, дает подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса и рассматривает вопросы обеспечения нормативно-распорядительной документацией и ресурсами и рекомендации по необходимым процедурам. Стандарт ГОСТ Р 53647 [2] содержит руководящие указания по внедрению системы менеджмента непрерывности бизнеса в организации, предназначен для организаций всех форм собственности и специалистов, ответственных за обеспечение непрерывности бизнеса организации.

Международные и национальные стандарты, например ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭ 27001:2005 [3], устанавливают требования к системе управления информационной безопасностью в целом, а также отдельно – к процессу управления инцидентами информационной безопасности. Данные стандарты обращают особое внимание на необходимость создания процесса управления инцидентами информационной безопасности и поддерживающей его работу документации, необходимой для регулирования и управления работой в рамках разработанного процесса и определения обязанностей, и необходимых действий сотрудников.

Технические рекомендации CMU/SEI-2004-TR-015 [4] описывают методологию планирования, внедрения, оценки и улучшения процессов управления инцидентами информационной безопасности. При этом основной упор делается на организацию работы группы или подразделения, обеспечивающего сервис и поддержку предотвращения, обработки и реагирования на инциденты информационной безопасности. Вводятся ряд критериев, на основании которых можно оценивать эффективность данных сервисов, приводятся подробные процессные карты.

Нормативный документ США NIST SP 800-61 [5] представляет собой сборник «лучших практик» по построению процессов управления инцидентами информационной безопасности и реагирования на них. Подробно разбираются вопросы реагирования на разные типы инцидентов, такие как атаки «отказ в обслуживании» (DoS), распространение вредоносного программного обеспечения, несанкционированный доступ, нерегламентированное использование и распределение, многокомпонентные атаки.

Международный стандарт ISO/IEC 27035:2011 [6] содержит структурированный и планомерный подход к обнаружению, составлению отчетов и оценке инцидентов информационной безопасности, к осуществлению ответной реакции и управлению инцидентами информационной безопасности, к обнаружению, оценке и устранению уязвимостей и к постоянному улучшению управления информационной безопасностью и инцидентами информационной безопасности.

В стандарте ISO/IEC 27031:2011 [7] содержатся концепции и принципы информационных и телекоммуникационных технологий как необъемлемой части критической инфраструктуры любой организации по обеспечению непрерывности ее бизнеса.

Британские стандарты серии BS 25999 [8] содержат общие рекомендации по управлению непрерывностью бизнеса, устанавливают

и детализируют конкретные требования к системам управления непрерывностью бизнеса, причем только те, соблюдение которых может быть объективно проверено.

Требования и рекомендации Стандарта Банка России СТО БР ИББС-1.0-2014 [9] направлены на минимизацию рисков возникновения инцидентов и снижения потерь от сбоев в работе. На базе этих требований можно построить программу обучения для студентов в высшем учебном заведении, а также управлять непрерывностью бизнеса для целей обеспечения непрерывности ключевых бизнес-процессов в рамках области действия системы управления информационной безопасностью. Стандарты в соответствии с лучшими практиками позволяют студентам убедиться в том, что процессы работают правильно и эффективно. Это особенно важно в том случае, если организация или государственный орган работает с большими объемами ценной информации или обрабатывает и хранит важную информацию своих клиентов и работников. При изучении стандартов полученный опыт рассматривается не только в рамках отдельного инцидента, но и проводится проверка на наличие тенденций (закономерностей) появления предпосылок к инцидентам, которые могут быть использованы в интересах определения потребности в защитных мерах или изменениях подходов к устранению инцидентов. После инцидента, связанного с применением информационных технологий, целесообразно проведение тестирования информационной безопасности, в особенности для оценки уязвимостей. Информация, получаемая в процессе инцидента, будет направляться для анализа тенденций (закономерностей), что на основе предшествующего опыта и документированных знаний в значительной мере способствует ранней идентификации инцидентов, а также обеспечивает предупреждение о том, какие инциденты могут возникнуть в будущем. Технологии эффективного функционирования системы для банковской сферы деятельности на основе стандартов по информационной безопасности, имеющие ярко выраженную специфику, описывает в своей работе С. В. Попов [10].

Кроме основ законодательства Российской Федерации, государственных стандартов в области информационных технологий (как отечественных, так зарубежных), студентов вуза необходимо обучать судебной практике в области расследования инцидентов информационной безопасности, а также программным продуктам для получения доказательной базы и документированию процесса управления инцидентами в целом. Благодаря этим знаниям и умениям обучающиеся смогут самостоятельно строить алгоритмы управления инцидентами информационной безопасности в организации. Например, с помощью стандарта ГОСТ Р ИСО/МЭК 18044-2007 [1] описывать систему управления инцидентами информационной безопасности. Анализировать этапы процесса управления инцидентами информационной безопасности, разбиваемого на планирование и подготовку, использование, анализ и улучшение относится к стандарту. Отдельно исследовать подпроцессы обнаружения событий и инцидентов информационной безопасности и оповещения о них, а также обработка событий и инцидентов информационной безопасности, включая первую оценку и предварительное решение по событию информационной безопасности и вторую оценку и подтверждение инцидента информационной безопасности. Для этого обучающиеся будут использовать ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭ 27001:2005 [3]. Детально исследовать подпроцесс реагирования на инциденты информационной безопасности и его составляющие будущим специалистам также позволит стандарт: немедленное реагирование, контроль, последующее реагирование, антикризисные действия, правовая экспертиза, передача информации, расширение области принятия решений, регистрация деятельности и контроль за внесением изменений и техническая поддержка реагирования на инциденты ИБ. Для разработки документации системы управления инцидентами информационной безопасности, включая политику и программу, используется ISO/IEC 27035:2011 [6].

Для обучения студентов анализу деятельности группы реагирования на инциденты информационной безопасности должен использоваться британский стандарт BS 25999. На его основе студенты осознают необходимость обеспечения осведомленности и обучения в области инцидентов информационной безопасности. Значительное внимание уделяется сохранению доказательств инцидента информационной безопасности и кратко определяются функции инструментальных средств управления событиями информационной безопасности.

Освоение этих материалов в учебном процессе лежит в основе формирования у об-

учающихся следующих профессиональных компетенций:

1) способность участвовать в управлении информационной безопасностью объекта (в части управления инцидентами информационной безопасности и непрерывностью бизнеса);

2) способность участвовать в проектировании и разработке системы управления информационной безопасностью (система управления информационной безопасностью) объекта (в отношении подсистем управления инцидентами информационной безопасности и непрерывностью бизнеса);

3) способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности система управления информационной безопасности объекта (в части эффективности и результативности управления инцидентами информационной безопасности и непрерывностью бизнеса).

Таким образом, управление инцидентами информационной безопасности является сложносоставным объектом изучения будущими специалистами по защите информации в вузе. Это – алгоритмический динамический объект, зависящий от постоянно меняющихся стандартов по управлению информационной безопасностью и по информационным технологиям, требующий разработки специальных обучающих методик, а потому – пристального внимания выпускающей кафедры.

Примечания

1. ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». М.: Стандартинформ, 2009.

2. ГОСТ Р 53647 «Менеджмент непрерывности бизнеса. Практическое руководство». М.: Стандартинформ, 2011.

3. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements» и ГОСТ Р ИСО/МЭ 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

4. CMU/SEI-2004-TR-015 «Defining incident management processes for CSIRT».

5. NIST SP 800-61 «Computer security incident handling guide».

6. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

7. ISO/IEC 27031:2011 «Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity».

8. BS 25999-1:2006 «Business continuity management. Code of practice» и BS 25999-2:2007 «Business continuity management. Specification».

9. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/Общие положения» принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399.

10. Попова С. В. Повышение эффективности функционирования системы мониторинга инцидентов информационной безопасности банка на основе оценки надежности ее компонентов: дис ... канд. техн.наук. – Тамбов, 2012. – 242 с.

Филиппов Андрей Сергеевич, аспирант кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: andr3yfilippov@yandex.ru

Астахова Людмила Викторовна, д. п. н., профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет, Челябинск. E-mail: lvastachova@mail.ru

Andrei Filippov, post-graduate student of the department of information systems security VPO «South Ural State University». E-mail: andr3yfilippov@yandex.ru

Lyudmila Astakhov, Professor, Department of «Security of information systems», South Ural State University, Chelyabinsk. E-mail: lvastahova@mail.ru

УДК 004.056.5 + 002 : 004.056 : 330.322

Чигринский Е. О.

ОЦЕНКА РИСКОВ И ИНВЕСТИРОВАНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЭКОНОМИЧЕСКОГО КРИЗИСА

Рассматривается влияние экономического кризиса на стратегию компаний в области информационной безопасности. Модернизируется методика оценки рисков путем введения новой переменной, отвечающей за кризисную ситуацию. Выделены предпосылки к дальнейшему изучению проблематики.

Ключевые слова: *информационная безопасность, экономический кризис, оценка рисков.*

Chigrinskiy E. O.

RISK MANAGEMENT AND INFORMATION SECURITY INVESTMENT DURING THE FINANCIAL CRISIS

There is a review of financial crisis impact on company's information security strategy. Risk analysis methodology was modified by introduction of new variable which considers the financial crisis. There are some prerequisites for the further issue study.

Keywords: *information security, financial crisis, risk management.*

Количество похищенной или скомпрометированной информации в мире выросло на 78%. В мире зафиксировано 1,5 тыс. утечек информации, итогом которых стала компрометация почти 1 млрд учетных данных. В 2014 году аналитическим центром InfoWatch зарегистрировано 1395 (3,8 в день, 116 в месяц) случаев утечки информации. Скомпрометированными оказалось 767 млн персональных данных (записей ПДн) – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация.

Средний ущерб, который наносит кража информации, оценивается в $25,51 млн. Такие данные приводятся в Индексе критичности утечек данных (BLI; Breach Level Index). Совокупный ущерб от утечек в мире, по данным Zecurion, составляет $17,782 млрд. Реальный ущерб подсчитать невозможно, так как все факты о хищениях информации собрать воедино практически нереально [1].

Все вышеприведенные факты могут быть связаны, в том числе, с финансовым кризисом. Эксперты полагают, что любая стагнация в эко-

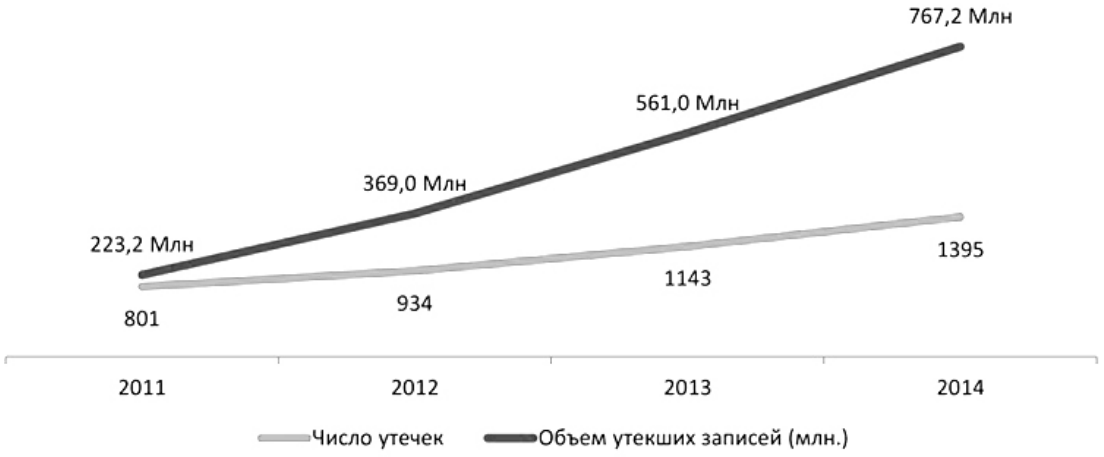

Рис. 1. Число утечек информации и объем утекших записей ПДн, скомпрометированных в результате утечек. 2011 - 2014 гг.

номике приводит к тому, что количество хищений данных из компании, увод клиентов, мошенничество многократно возрастают. Тайно работая на компанию-конкурента, недобросовестные сотрудники просто подстраховываются от возможных финансовых трудностей.

Многие компании выстраивают свою стратегию защиты информации на основе тех данных, которые были получены в результате оценки рисков информационной безопасности (ИБ). Такой порядок действий логичен и обоснован, риск-менеджмент использует существующие методики и ожидает соответствующих результатов. Тем не менее, согласно приведенным исследованиям, объем потерь не только не сокращается, но и, более того, растет. В таком случае мы можем поставить под сомнение точность существующих методов оценки рисков с учетом явного роста статистики случаев хищения и утечки данных. Можно предположить, что появился некий не учитываемый ранее фактор, влияющий на прогнозы оценочных методов, который может вносить свои коррективы.

И действительно, на данный момент не существует методик оценки рисков ИБ таких, которые бы учитывали динамические факторы. А именно такие факторы, которые могут появиться в любой момент времени, в зависимости от состояния окружающей среды и/или изменения некоторой ситуации в частности. Прогнозирование таких факторов – чрезвычайно сложная задача. Однако невозможно не признать, что производить расчет информационных рисков безотносительно всякого учета неожиданного появления новых факторов, способных повлиять на уровень информационного риска в целом, было бы недальновидно. Учитывая текущую ситуацию в стране, на данный момент нас интересует фактор экономического кризиса.

На примере метода оценки рисков ИБ на предприятиях малого и среднего бизнеса рассмотрим включение корректирующего фактора в формулу расчета риска реализации угроз [2]. Алгоритм оценки методики с учетом корректировки, затрагивающей экономический фон, представлен на рис. 2.

Рис. 2. Алгоритм оценки рисков информационной безопасности

Шаг 1. Идентификация активов. Руководители отделов и подразделений совместно со специалистами по информационной безопасности определяют все ресурсы, которые имеют ценность или находят полезное применение в организации, обеспечивают непрерывность ее деловых операций.

Шаг 2. Определение риска от кредитного рейтинга. Кредитный рейтинг — мера кредитоспособности частного лица, компании, региона или страны. Кредитные рейтинги рассчитываются на основе прошлой и текущей финансовой истории вышеперечисленных участников рынка, а также на основе оценок размера их собственности и взятых на себя финансовых обязательств. Кредитные рейтинги относительны, поэтому важно учитывать специфику той или иной страны, предприятия, отрасли промышленности. Невысокие кредитные рейтинги, конечно, нежелательны, ибо свидетельствуют о высокой вероятности дефолта [3]. Крупнейшими рейтинговыми агентствами (которые работают во всем мире) являются Moody's, Standard and Poor's и Fitch Ratings. Их системы оценок представлены в таблице 1. Все эти агентства понизили индекс кредитного рейтинга России в 2014 году из-за экономических санкций, замедления темпов экономического роста и сложной геополитической ситуации между

Таблица 1. Показатели рейтингов крупнейших кредитных агентств

<table>
<tr><th colspan="3">Индекс кредитного рейтинга</th><th rowspan="2">Характеристика</th></tr>
<tr><th>Moody's</th><th>S&P</th><th>Fitch</th></tr>
<tr><td>Aaa</td><td>AAA</td><td>AAA</td><td>Обязательства наивысшего качества</td></tr>
<tr><td>Aa1</td><td>AA+</td><td>AA+</td><td rowspan="3">Обязательства высокого качества</td></tr>
<tr><td>Aa2</td><td>AA</td><td>AA</td></tr>
<tr><td>Aa3</td><td>AA-</td><td>AA-</td></tr>
<tr><td>A1</td><td>A+</td><td>A+</td><td rowspan="3">Обязательства выше среднего качества</td></tr>
<tr><td>A2</td><td>A</td><td>A</td></tr>
<tr><td>A3</td><td>A-</td><td>A-</td></tr>
<tr><td>Baa1</td><td>BBB+</td><td>BBB+</td><td rowspan="3">Обязательства ниже среднего качества</td></tr>
<tr><td>Baa2</td><td>BBB</td><td>BBB</td></tr>
<tr><td>Baa3</td><td>BBB-</td><td>BBB-</td></tr>
<tr><td>Ba1</td><td>BB+</td><td>BB+</td><td rowspan="3">Рискованные обязательства с чертами спекулятивных</td></tr>
<tr><td>Ba2</td><td>BB</td><td>BB</td></tr>
<tr><td>Ba3</td><td>BB-</td><td>BB-</td></tr>
<tr><td>B1</td><td>B+</td><td>B+</td><td rowspan="3">В высокой степени спекулятивные</td></tr>
<tr><td>B2</td><td>B</td><td>B</td></tr>
<tr><td>B3</td><td>B-</td><td>B-</td></tr>
<tr><td>Caa1</td><td>CCC+</td><td rowspan="5">CCC</td><td>Очень высокий кредитный риск</td></tr>
<tr><td>Caa2</td><td>CCC</td><td>Крайне спекулятивные</td></tr>
<tr><td>Caa3</td><td>CCC-</td><td rowspan="3">Близки к дефолту</td></tr>
<tr><td rowspan="2">Ca</td><td>CC</td></tr>
<tr><td>C</td></tr>
<tr><td>C</td><td rowspan="3">D</td><td>DDD</td><td rowspan="3">В состоянии дефолта</td></tr>
<tr><td>/</td><td>DD</td></tr>
<tr><td>/</td><td>D</td></tr>
</table>

Россией и Украиной. При присвоении рейтинга финансовому институту учитывается следующее:

• Экономические риски – сильные и слабые стороны экономической и политической ситуации в стране (размер экономики, ее состав, перспективы развития), а также какие эффекты (как прямые, так и косвенные) они могут оказать на банковский/финансовый сектор в стране – изменение процентной ставки, спроса на кредиты и др.

• Риски внутри сектора – уделяется отдельное внимание размеру банковского сектора в стране, его структура, его административное регулирование, количество агентов, прозрачность, процент фондов в экономике, проходящих через сектор, динамики конкуренции, барьеры на входе, количество банков и дочерних компаний, иностранное присутствие в данном секторе экономики.

• Ситуация на рынке – положение оцениваемого банка на рынке. Выводы делаются на основании уровня рыночной власти, диверсификации, стратегии, управления рисками, клиентской базы и др. [4].

Таким образом, кредитный рейтинг наглядным образом отражает изменения в экономике предприятия или страны и не остается без внимания при надвигающемся или наступившем экономическом кризисе (Табл. 1).

Риск, связанный с экономической обстановкой в стране, влияет на общий риск информационной безопасности компании. Если рассматриваемая компания фигурирует в рейтинге одного из представленных агентств, то следует брать ее соответствующий показатель для определения значения риска согласно таблице 2. Это даст более точные конечные результаты. В противном случае берется рейтинг страны в целом, в которой осуществляется бизнес. Также возможен вариант, при котором выставить рейтинг предприятия могут собственные эксперты в экономической сфере.

К примеру, мы определяем риск реализации угрозы для ОАО «РЖД». На этом шаге нам нужно определить коэффициент кредитного рейтинга. В январе 2015 года рейтинговое агентство Fitch Ratings присвоило им индекс кредитного рейтинга, равный «BBB-», что является по таблице 1 «обязательством ниже среднего качества». Согласно таблице 2 коэффициент кредитного рейтинга ОАО «РЖД» будет равняться 0,4.

Таблица 2. Определение коэффициента кредитного рейтинга.

Категория кредитного рейтинга	Коэффициент кредитного рейтинга (R_k)
Обязательства наивысшего качества	0,1
Обязательства высокого качества	0,2
Обязательства выше среднего качества	0,3
Обязательства ниже среднего качества	0,4
Рискованные обязательства с чертами спекулятивных	0,5
В высокой степени спекулятивные	0,6
Очень высокий кредитный риск	0,7
Крайне спекулятивные	0,8
Близки к дефолту	0,9
В состоянии дефолта	1

Шаг 3. Разработка модели угроз. Необходимо разработать частную модель угроз информационной безопасности экспертным составом специалистов в области защиты информации, в которой также определяется актуальность угроз ИБ. Затем составляется перечень актуальных угроз на каждый выделенный актив из вышеупомянутого шага с определением вероятности реализации угрозы.

Шаг 4. Процедура количественной оценки рисков. Данная процедура включает в себя следующие этапы: выбор актуальных угроз частной модели угроз, определение вероятности наступления угрозы, определение ценности актива, определение возможности использования организационных и технических уязвимостей, вычисление численного значения риска.

Вероятность реализации угрозы на актив равна разности между единицей и произведением вероятностей противоположных событий.

Как правило, точную ценность актива определить достаточно сложно либо совсем невозможно, поэтому рекомендуется присваивать ему значение от 0 до 1, исходя из того, какое соотношение цены актива к стоимости всего бизнеса. На этом этапе в состав экспертной комиссии рекомендуется включать руководителя компании.

Соответствие выполняемых организационных и технических мер по защите информации к коэффициентам организационных и технических уязвимостей представлены в таблицах 3 и 4 соответственно.

Таблица 3. Определение коэффициента организационных уязвимостей

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_0)
14–17	0,01
8–13	0,25
менее 8	0,5
не выполняются	0,9

Таблица 4. Определение коэффициента технических уязвимостей

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_t)
15–19	0,01
сен. 14	0,25
менее 9	0,5
не выполняются	0,9

Формула (1) расчета риска реализации хотя бы одной угрозы из перечня определенных актуальных угроз с учетом наличия уязвимостей по отношению к конкретному активу выглядит следующим образом:

$$R = P_{\text{угр}} R_k C \frac{K_0 + K_t}{2} 100\%, \qquad (1)$$

где R – численная величина риска реализации угроз ИБ; $P_{\text{угр}}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз; R_k – коэффициент кредитного рейтинга; C – ценность актива; K_0 – вероятность использования организационных уязвимостей; K_t – вероятность использования технических уязвимостей.

Допустимым принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для компаний малого и среднего бизнеса рекомендованное значение не должно превышать 5%. Считается, что реализация актуальной угрозы, повлекшей ущерб более 5% выручки за отчетный период (1 год), является неприемлемым и требуется принятие эффективных мер.

Заключение

При внедрении переменной R_k, отвечающей за изменения экономического фона на предприятии или в стране, где ведется бизнес, результаты проведения оценки риска для важных активов станут более точными и позволят более гибко реагировать на экономические колебания. Абсолютно все факторы учесть очень сложно или практически невозможно, но стремиться к этому стоит при корректировке существующих методик или создании новых. В конечном итоге действенность любого метода доказывается на практике. Наблюдение эффекта, оказываемого на общий расчет введением такого коэффициента, а также его влияние на выбор стратегии ИБ и финальный результат планируются к дальнейшему рассмотрению. Идеальным итогом в последующем развитии работы над данной проблематикой было бы создание динамической модели, которая будет учитывать в себе изменения различных внешних факторов, влияющих на конечный результат определения показателя информационного риска в режиме реального времени. Это существенно снизит убытки компаний и позволит оперативно реагировать на изменения внешней среды.

Примечания

1. Как кризис влияет на количество инцидентов ИБ // Портал СмартСорсинг. URL: http://smartsourcing.ru/blogs/informatsionnaya_

2. bezopasnost/2791/ (дата обращения: 29.04.2015).

3. Плетнев П. В., Белов В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа. – № 1(25), 2012. – С. 83–86.

4. Международный кредитный рейтинг // Портал Кредиты 2014. URL: http://itb2014.org/международный-кредитный-рейтинг/ (дата обращения: 29.04.2015).

5. Титкова Е. С. Методика формирования финансовых рейтингов // Мировое и национальное хозяйство. 2011. – № 4(19).

Чигринский Евгений Олегович, главный специалист отдела защиты информации МБУ «Электронный Екатеринбург», г. Екатеринбург. E-mail: echigrinskiy@gmail.com

Chygrynskiy Eugene, chief specialist of information protection MBU «Electronic Yekaterinburg», Yekaterinburg. E-mail: echigrinskiy@gmail.com

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ «ВЕСТНИК УрФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ»

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцом оформления рукописи, а также приложить к статье сведения о себе (см. Сведения об авторе).

Сведения об авторе

ФИО (полностью)	
Ученая степень	
Ученое звание	
Должность и место работы (полностью)	
Домашний адрес	
Контактные телефоны	
e-mail	
Тема статьи	
Являетесь ли аспирантом (если да, то указать дату приема в аспирантуру и научного руководителя)	

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

Структура статьи (суммарный объем статьи – не более 40 000 знаков):

1. УДК, ББК, название (не более 12–15 слов), список авторов.
2. Аннотация (не более 500 знаков, включая пробелы), список ключевых слов.
3. Основной текст работы.
4. Примечания.

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 до 50 слов, ниже отдельной строкой — ключевые слова. Инициалы и фамилия автора (авторов), название статьи, аннотация и ключевые слова должны быть переведены на английский язык.

В случае непрямого цитирования источников и литературы в начале соответствующего примечания указывается «См.:».

Цитируемая литература дается не в виде подстрочных примечаний, а общим списком в конце статьи с указанием в тексте статьи ссылки порядковой надстрочной цифрой (Формат — Шрифт — Надстрочный) (например, [1]). Запятая, точка с запятой, двоеточие и точка ставятся после знака сноски, чтобы показать, что сноска относится к слову или группе слов, например: по иску собственника[1]. Вопросительный, восклицательный знак, многоточие и кавычки ставятся перед знаком сноски, чтобы показать, что сноска относится ко всему предложению, например: …все эти положения закреплены в Федеральном законе «О ветеранах»[1].

Литература дается в порядке упоминания в статье.

При подготовке рукописи автору рекомендуется использовать ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (Полный текст ГОСТ Р размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии).

В конце статьи 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.

Обязательно для заполнения: В конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — ученая степень, ученое звание, должность, кафедра, вуз; рабочий адрес, электронный адрес и контактные телефоны.

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Информационная безопасность.

Порядок прохождения рукописи

1. Все поступившие работы регистрируются, авторам сообщается ориентировочный срок выхода журнала, в макет которого помещена работа.

2. Поступившая работа проверяется на соответствие всем формальным требованиям и при отсутствии замечаний, в случае необходимости, направляется на дополнительную экспертизу.

3. Для публикации работы необходима положительная рецензия специалиста из данной или смежной области. На основании рецензии принимается решение об опубликовании статьи (рецензия без замечаний) или о возврате автору на доработку, в этом случае рукопись может проходить экспертизу повторно. При получении второй отрицательной рецензии на работу редакция принимает решение об отказе в публикации.

Материалы к публикации отправлять по адресу

E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО».

Или по почте по адресу:

Россия, 454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(15) / 2015

Дата выхода в свет 30.03.2015. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,6. Тираж 100 экз. Заказ 385/454.
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. 1(15) / 2015

Date of publication of the 30.03.2015. Format 70×108 1/16. Screen printing.
Conventional printed sheet 5,6. Circulation – 100 issues. Order 385/454. Open price.

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