

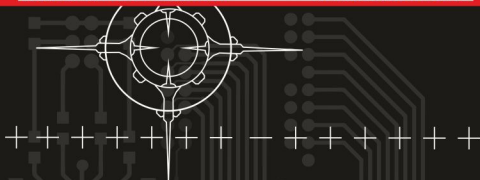
ISSN: 2311-3456

# ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№2 2014  
(3)

VOPROSY KIBERBEZOPASNOSTI

CYBERSECURITY ISSUES



Централизованные системы кибербезопасности

Стенографические системы связи

Программно-аппаратные закладки



# О ПОДХОДАХ К РЕАЛИЗАЦИИ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ АСУ ВОЕННОГО И СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

*Бородакий Юрий Владимирович, академик РАН, доктор технических наук, профессор  
Добродеев Александр Юрьевич, кандидат технических наук, старший научный сотрудник  
Нащекин Павел Александрович  
Бутусов Игорь Викторович*

*В статье рассматриваются актуальные практические подходы к реализации централизованной системы управления информационной безопасностью современных автоматизированных систем управления военного и специального назначения. Предложены перспективные элементы и комплексы средств защиты информации и возможные направления развития систем комплексной защиты информации.*

**Ключевые слова:** информационная безопасность, система управления, комплексная защита, средства защиты информации.

## THE APPROACH TO IMPLEMENTING A CENTRALIZED SYSTEM FOR INFORMATION SECURITY MANAGEMENT AS MP

*Yuri Borodakiy, Member of the RAS,  
Doctor of Technical Sciences, Professor  
Alexander Dobrodeyev, Ph.D., Associate Professor  
Pavel Nashchekin  
Igor Butusov*

*The practical implementation of a centralized system for information security management of modern automated systems of military and special purpose is discussed. The promising elements and complexes of information security and possible directions of development of integrated systems of information protection are offered.*

**Keywords:** information security, management system, comprehensive protection, information security tools.

Непрерывное совершенствование информационных технологий, повышение их роли и значимости, расширение сферы применения автоматизированных систем управления военного и специального назначения (АСУ ВиСН) в процессах управления государством и его Вооруженными Силами требуют постоянного внимания к вопросам обеспечения их информационной безопасности.

Обеспечение информационной безопасности АСУ ВиСН представляет собой комплексную проблему, которая решается в направлениях нормативного и правового регулирования применения АСУ ВиСН, совершенствования методов и средств

их разработки, развития системы оценки соответствия требованиям информационной безопасности, обеспечения соответствующих организационно-технических условий безопасной эксплуатации, включая управление системой обеспечения безопасности обрабатываемой информации.

В России сложилась и определенным образом реализуется система обеспечения информационной безопасности АСУ ВиСН. Основы функционирования этой системы определяются Федеральными законами, Указами Президента Российской Федерации, руководящими и методическими документами федеральных органов исполнительной власти, относящимися к сфере

информационных технологий и информационной безопасности.

Вместе с тем, в настоящее время противоборствующими сторонами активно развивается широкий спектр новых методов и технологий информационного воздействия как на отдельные средства вычислительной техники (СВТ), так и на информационно-телекоммуникационные системы (ИТС) и АСУ органов государственного и военного управления, реализация которых направлена на получение несанкционированного доступа к информационным ресурсам и нарушение их функциональной устойчивости. Усилено ведется разработка новых информационных технологий для проведения информационных атак на АСУ ВиСН, постоянно совершенствуется уже существующие и появляются новые способы и средства проведения атак, а число компьютерных инцидентов ежегодно увеличивается.

При этом АСУ ВиСН рассматриваются в качестве одного из основных приоритетных объектов комплексного деструктивного воздействия, направленного на завоевание информационного превосходства и нарушение (затруднение) управления. В этих условиях проблема обеспечения информационной безопасности в различных условиях обстановки становится одной из ключевых в решении задач построения АСУ ВиСН [1-6].

В соответствии с Доктриной информационной безопасности Российской Федерации угрозами безопасности АСУ ВиСН, как уже развернутых, так и создаваемых на территории России, могут являться:

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи АСУ ВиСН;

- несанкционированный доступ к информации (НСД), циркулирующей в АСУ ВиСН, а так же находящейся в банках и базах данных;

- противоправные сбор и использование информации, циркулирующей в АСУ ВиСН;

- нарушение технологии обработки информации;

- утечка информации по техническим каналам;

- воздействие на парольно-ключевые системы автоматизированных систем обработки и передачи информации;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи;

- компрометация ключей и средств криптографической защиты информации, а также сервисов и инфраструктуры электронной подписи;

- разработка и распространения вредоносных программ, нарушающих функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации, а также программ сбора информации об объектах информатизации;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрирование этой информации и навязывание ложной информации;

- использование несертифицированных по требованиям безопасности информации отечественных и зарубежных информационных технологий, средств защиты информации и контроля доступа виртуализации, средств информатизации, телекоммуникации и связи и т.д.

Вместе с тем, развитие информационных и коммуникационных технологий вызвало возникновение ряда новых и развитие некоторых существующих угроз информационной безопасности, таких как [2, 3, 7-9]:

- деструктивные информационно-технические воздействия (в том числе применение кибероружия, средств радиоэлектронной борьбы (РЭБ), проникновение в компьютерные сети) на информационно-технические объекты АСУ ВиСН;

- компьютерные атаки на информационные сегменты АСУ ВиСН (информационно-коммуникационные, функциональные, информационно-психологические и др.);

- преднамеренные действия, а также ошибки персонала и диверсионно-подрывная деятельность специальных служб иностранных государств;

- электромагнитный терроризм;

- внедрения в аппаратные и программные изделия АСУ ВиСН компонентов, реализующих функции, не предусмотренные документацией на эти изделия (НДВ);

- использование базы данных скомпрометированных идентификаторов;

- доступ к ресурсам неавторизованных пользователей по действующим аппаратным идентификаторам (смарт-карты, токены и т.п.);

- подмена «облачной» инфраструктуры обработки информации;

- активация служебных режимов функционирования изделия путем получения специальных команд (поток) при штатной обработке информации;

- обеспечение функционирования СВТ под управлением недоверенного гипервизора и т.д.

Основой построения перспективных современных АСУ ВиСН, соответствующим высоким

требованиям к их функциональным возможностям, надежности и функциональной устойчивости в условиях современного информационного противоборства является использование при их построении доверенной программно-аппаратной платформы (среды) [7, 9]. При этом реализация требований доверенности к аппаратной среде предполагает:

- применение основных и вспомогательных технических средств, прошедших специальную проверку и специальные исследования и получивших заключение о спецпроверке и предписание на эксплуатацию;

- обязательную сертификацию по требованиям безопасности информации к средствам вычислительной техники (СВТ) по требуемому классу защиты всех технических средств (составных частей) из состава изделия (системы специального назначения);

- использование аппаратных средств защиты информации (СрЗИ) российской разработки, прошедших сертификационные исследования программных средств на отсутствие недеclared возможностей и безопасность исходных кодов, а также подтверждение реально декларированных возможностей;

- использование сертифицированных активных и пассивных технических средств защиты

информации (генераторы шума, фильтры, экраны и т.д.).

Классический подход к созданию современных систем защиты информации (СЗИ) и обеспечению информационной безопасности изделий и объектов эксплуатации показан на рисунке 1.

Опыт разработок ОАО «Концерн «Системпром» АСУ в защищенном исполнении показывает, что основу защиты АСУ ВиСН от НСД должен составлять программно-аппаратный комплекс СЗИ от НСД, составляющими компонентами которого являются аппаратно-программный модуль доверенной загрузки (АПМДЗ) и программное изделие СЗИ от НСД, построенное из следующих функциональных модулей (технологий защиты): разграничения доступа; контроля и управления профилями; управления и регистрации печати; паролирования; антивирусной защиты; тестирования и экстренного уничтожения информации; системы мониторинга и управления событиями безопасности, усиления идентификации и аутентификации с использованием биометрических средств; комплексы «прозрачного» взаимодействия с разнокатегорированными информационными ресурсами.

Модульный подход к созданию систем защиты информации позволяет строить системы защиты требуемого Заказчику класса защищенности.

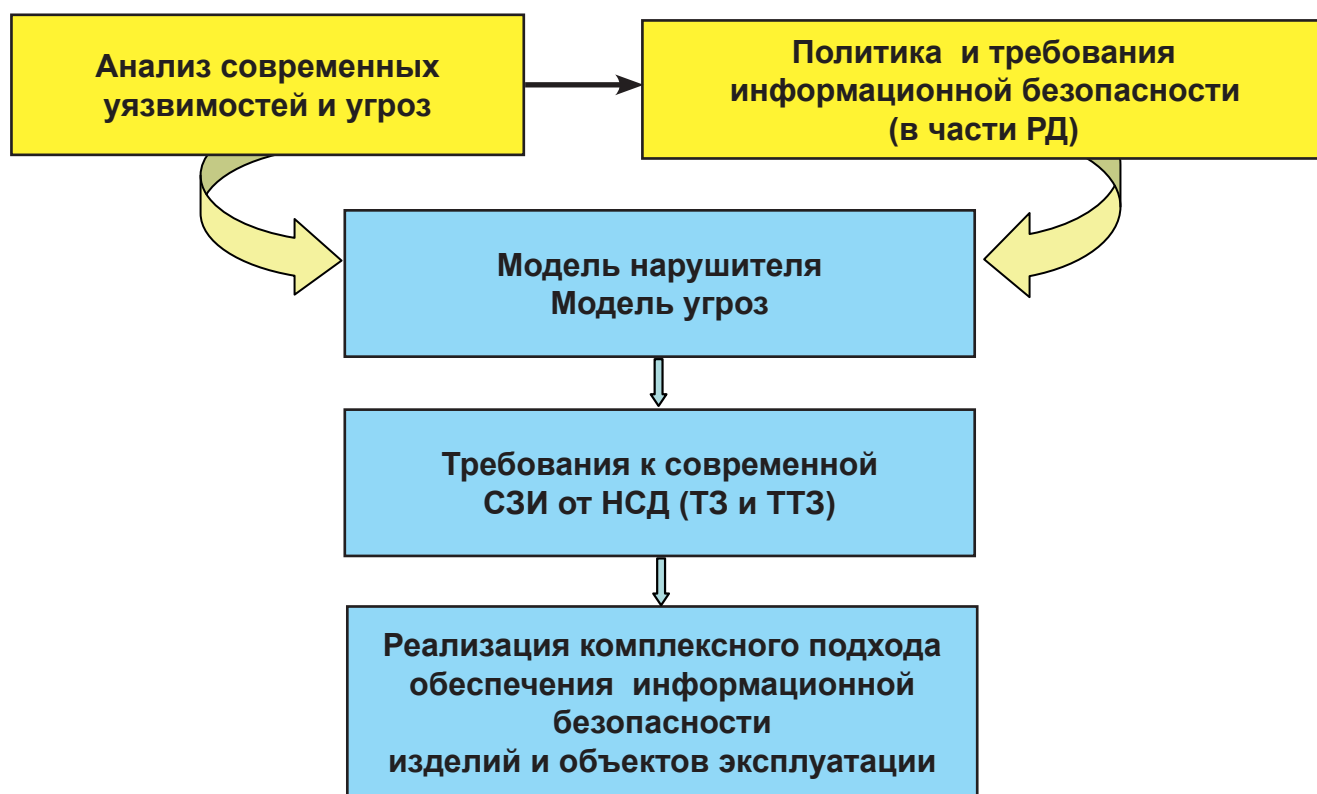


Рис.1. Классический подход к созданию современных СЗИ и обеспечению информационной безопасности изделий и объектов эксплуатации



Аналогичный модульный подход может применяться так же для построения системы комплексной защиты информации [10].

Важным критерием реализации ПАК СЗИ от НСД является обеспечение защищенной замкнутой программно-аппаратной среды с реализацией возможности централизованного и интерактивного контроля защищенности АСУ, а также управление всеми элементами СЗИ в АСУ и управления событиями безопасности, включая функциональный контроль.

Особую роль в обеспечении высоких классов защиты распределенных АСУ ВиСН играет разумная реализация системы (подсистемы) криптографической защиты информации. Ее состав и особенность построения и реализации (интеграции) - отдельный вопрос рассмотрения, следует упомянуть несколько слов об основных задачах, на решение которых направлена система (подсистема) криптографической защиты информации: идентификация и аутентификация пользователей; шифрование информации (трафика) в сети; шифрование информации на отчуждаемых и встраиваемых (внутренних) носителях; поддержка инфраструктуры электронной подписи; обеспечение ряда требований руководящих документов в части НСД (регистрация, управление печатью и т.д.).

Следует отметить, что основной особенностью современного этапа в создании защищенных систем является то, что мы находимся на этапе некоторой технической революции, когда на смену дорогой, громоздкой низкоскоростной аппаратуре ЗАС приходят современные высокоскоростные средства шифрования и средства криптографической защиты информации, такие как, IP и Ethernet - шифраторы, криптошлюзы и криптомаршрутизаторы на их основе, масштабируемые криптографические пулы с автоматизированной балансировкой нагрузки.

Разумное применение данных изделий позволяет строить защищенные системы со значительно большими функциональными возможностями и более высокими вероятностно-временными характеристиками. Стремительное развитие компьютерной техники, ее функциональных возможностей закономерно вызвало бурное развитие и разработку новых криптографических средств защиты информации для защиты от НСД самих автоматизированных рабочих мест (АПМДЗ, шифраторы носителей, подключаемых по интерфейсам USB и eSATA, функции однонаправленного ввода информации с отчуждаемых носителей, обеспечение доверенной виртуализации) и сетевого трафика внутри локальной сети и комплекса средств автоматизации (КСА).

Обязательным условием является применение только сертифицированных по требованиям безопасности информации средств и систем. При этом, основными компонентами СЗИ являются системы защиты информации телекоммуникационных сетей, системы защиты информации локальных вычислительных сетей и системы защиты информации АРМ и серверов (рис.2).

Особенностью современного этапа развития информационно-управляющих систем специального назначения (ИУС СН), к числу которых относится АСУ ВиСН, является всё более глубокая интеграция взаимодействующих систем и наполнение их новыми сервисами благодаря внедрению перспективных технологий.

При этом на первый план выходят следующие задачи:

- объединение информационных ресурсов взаимодействующих систем;
- обеспечение виртуализации вычислений с высоконадежной миграцией данных и виртуальных машин;
- реализация специального программного обеспечения (СПО) в виде сервисов и миграции СПО под различные операционные системы;
- создание общей доверенной среды обмена данными взаимодействующих ИУС СН;
- реализация иерархической системы взаимодействующих удостоверяющих центров взаимодействующих ИУС СН;
- переход на новую аппаратно-вычислительную базу;
- совершенствование технологий работы с электронной подписью в свете перехода на новую нормативную базу.

Соответственно в рамках взаимодействующих систем и изменения условий функционирования ИУС СН возникает необходимость реализации системы управления информационной безопасностью.

При этом в качестве перспективных решений целесообразно рассматривать:

- реализацию адаптивной централизованной системы управления информационной безопасностью ИУС СН с применением унаследованных и перспективных решений в области защиты информации;
- реализацию системы комплексной защиты информации на новых технических решениях;
- совершенствование нормативно-методической базы с учётом внедрения в ИУС СН новых технологий обработки информации и защиты.

Учитывая комплексность применения технических решений особую актуальность приобретает задача обеспечения централизованного управления системой комплексной защиты информации в

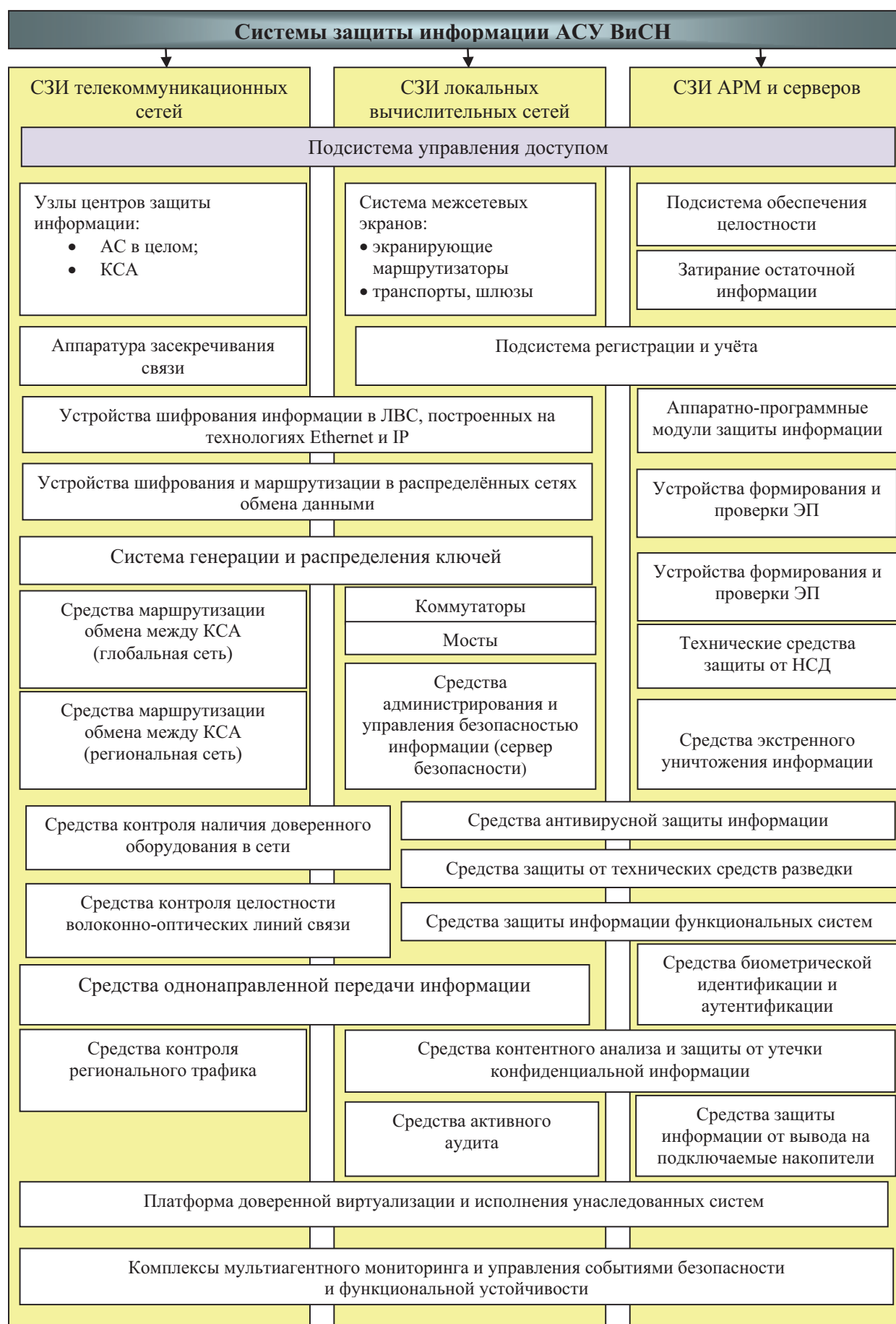


Рис. 2. Основные компоненты систем защиты информации АСУ ВиСН

рамках как одной ИУС СН, так и взаимодействующих (ресурсных) систем, с обеспечением следующих основных функций:

контроль защищенности и соответствия заданной топологии;

управление начальной настройкой программных средств СЗИ;

корректировка параметров идентификации и полномочий субъектов доступа к защищаемым ресурсам с учетом централизованной базы актуализации эталонных биометрических образов;

оповещение администратора безопасности информации о попытках НСД к защищаемым ресурсам с реализацией возможности не только локализации точек воздействия, но и с автоматизированным предоставлением сценария противодействия и фиксацией улик действий нарушителя;

управление блокировкой (разблокировкой) технических средств для локализации последствий НСД;

стирание информации в запоминающих устройствах;

создание (определение) защищенных областей магнитных носителей, каталогов, подкаталогов;

контроль за сохранностью (неизменностью, целостностью) информационного обеспечения, в том числе средств защиты, отображение результатов контроля;

архивирование и восстановление информации базы данных безопасности;

ведение журналов регистрации и учета информации на отчуждаемых носителях, ее архивации, просмотра и получение справок;

генерация паролей в соответствии с криптографическими и инженерно-криптографическими требованиями;

централизованное управление средствами антивирусной защиты, а так же изоляция (блокировка) АРМ должностных лиц, на которых выявлена вирусная активность.

Вместе с тем, в условиях взаимодействующих систем целесообразно отдельно выделить проблемы практической реализации централизованного управления средствами систем комплексной защиты информации в рамках нескольких взаимодействующих систем, в процессе которого должны быть реализованы следующие возможности:

реализация централизованной системы управления информационной безопасностью;

централизованное и сетевое управление криптографической подсистемой (настройка, распределение ключей, смена ключей);

централизованное управление подсистемой антивирусной защиты (обновление версий САВЗ и баз вирусных сигнатур, удаленный контроль);

автоматизированный контроль защищенности объектов ИУС СН;

автоматизированный контроль защищенности объектов взаимодействующих ИУС СН на основе мультиагентной системы;

интеграция с техническими средствами охраны и средствами контроля и управления доступом, а так же системами химической, биологической и радиационной безопасности и системой видеонаблюдения;

контроль защищенности от технических средств разведки;

организация однонаправленного ввода информации в ИУС СН;

обеспечение возможности работы должностных лиц в контурах с различной категорией обрабатываемой взаимодействующими системами информации;

обеспечение возможности интерактивного получения информации из разнокатегорированных систем;

автоматизированный прогноз защищенности совокупности взаимодействующих систем в условиях плановой эволюции.

Централизованная систем управления должна охватывать как унаследованные, хорошо себя зарекомендовавшие в условиях реальной эксплуатации, технические решения, так и перспективные, разрабатываемые в настоящее время элементы и комплексы средств защиты информации.

В качестве перспективных элементов и комплексов средств защиты информации целесообразно рассматривать:

- унифицированные аппаратно-программные модули доверенной загрузки с функциями управления по сети ИУС СН, обеспечения доверенной виртуализации и контроля отчуждаемых носителей информации;

- программно-аппаратные комплексы защиты информации от информационно-технического воздействия;

- комплексы защиты информации технологии «тонкий клиент» и средств виртуализации;

- высокопроизводительные криптографические средства защиты информации, включая криптографические пулы;

- программные комплексы централизованного управления средствами защиты информации взаимодействующих ИУС СН в рамках одной мультиплатформенной системы управления информационной безопасностью (СУИБ);

- средства защиты от НСД к вычислительным ресурсам центров обработки данных (ЦОД) на базе Blade-серверов и средства оперативной миграции виртуальных машин и серверов;

- автоматизированные средства построения ложных объектов;
- средства взаимодействия с несколькими удостоверяющими центрами;
- средства централизованной биометрической идентификации и аутентификации.

Современные тенденции развития ИУС СН требуют при создании АСУ ВиСН учитывать следующие перспективные направления развития систем комплексной защиты информации[4]:

разработку средств защиты информации распределённых вычислений и услуг ЦОД («облачные вычисления»);

реализацию криптографических сервисов для распределённых вычислений [5];

обеспечение централизованного управления инфраструктурой электронной подписи с учетом построения доверенного пространства многоуровневой системы удостоверяющих центров;

реализацию технологии интеграции АС, основанной на интеграции сервисов с предоставлением возможностей виртуализации выносных, рабочих мест, серверных компонентов и электронного документооборота, включающего обработку потоков документов, заданий, индексацию и поиск информации (Интеграционный комплекс информационно сетевых сервисов (ИКИСС);

реализацию автоматизированных средств (сервисов) оценки эффективности защиты взаимодействующих ИУС СН;

защиту информации, обрабатываемой средствами виртуализации, в том числе с использованием виртуальных средств организации взаимодействия между сегментами АСУ (виртуальная сетевая инфраструктура, рабочие места и вычислительные комплексы);

централизованное управление персональными биометрическими данными для доступа к ресурсам АС, а так же на объекты охраны;

реализацию возможностей централизованного управления гетерогенными СЗИ взаимодействующих ИУС СН в рамках единой СУИБ;

построение системы компетенций СЗИ и системы взаимного доверия сервисов взаимодействующих ИУС СН;

криптографическую защиту информации при передаче по беспроводным каналам связи, включая мобильные устройства и оконечные исполнительные устройства;

внедрение перспективных средств идентификации абонентов и носителей ключевой информации и др.

Таким образом, только на основе реализации комплексного подхода в обеспечении информационной безопасности на основе перечисленных технологий и механизмов защиты может быть достигнут требуемый высокий уровень информационной безопасности, надежности и функциональной устойчивости АСУ ВиСН в условиях современного информационного противоборства.

## Литература

1. Бородакий Ю.В., Боговик А.В., Карпов Е.А., Курносков В.И., Лободинский Ю.Г., Масановец В.В., Парашук И.Б. Основы теории управления в системах специального назначения. Учебник. М.: Изд. Управление делами Президента Российской Федерации, 2008. 306 с.
2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
3. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) // Вопросы кибербезопасности. 2014. № 1 (2). С. 5-12.
4. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Предложения в межведомственную концепцию создания доверенной аппаратно-программной среды для автоматизированных систем органов управления // Вопросы радиоэлектроники. 2013. Т. 3. № 2. С. 15-22.
5. Бородакий Ю.В., Добродеев А.Ю., Свиридюк Ю.П., Нащёкин П.А. Основные задачи и проблемы

## References

1. Borodakiy Yu.V., Bogovik A.V., Karpov Ye.A., Kurnosov V.I., Lobodinskiy Yu.G., Masanovets V.V., Parashchuk I.B. Osnovy teorii upravleniya v sistemakh spetsialnogo naznacheniya. Uchebnik, Moscow, Izd. Upravleniye delami Prezidenta Rossiyskoy Federatsii, 2008, 306 p.
2. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti, 2013, No 1(1), pp.2-9.
3. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 2), Voprosy kiberbezopasnosti, 2014, No 1 (2), pp. 5-12.
4. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Predlozheniya v mezhdvedomstvennuyu kontseptsiyu sozdaniya doverennoy apparatno-programmnoy sredy dlya avtomatizirovannykh sistem organov upravleniya, Voprosy radioelektroniki, 2013, Vol. 3, No 2, pp. 15-22.
5. Borodakiy Yu.V., Dobrodeyev A.Yu., Sviridyuk Yu.P., Nashchekin P.A. Osnovnyye zadachi i problemy

- создания криптографической подсистемы защиты распределённых автоматизированных систем управления и связи специального назначения // Информационное противодействие угрозам терроризма. 2005. № 4. С. 176-178.
6. Бородакий Ю.В., Лободинский Ю.Г. Информационные технологии в военном деле (основы теории и практического применения). М.: Горячая линия - Телеком, 2008. 392 с.
7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность - подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22-27.
8. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С. 10-16.
9. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1(2). С. 13-21.
10. Соснин Ю.В., Куликов Г.В., Непомнящих А.В., Нащёкин П.А. Базовые технологии моделирования процедур защиты информации от несанкционированного доступа // Вопросы защиты информации. 2014. № 1 (104). С. 23-28.
- sozdaniya kriptograficheskoy podsistemy zashchity raspredelennykh avtomatizirovannykh sistem upravleniya i svyazi spetsialnogo naznacheniya, Informatsionnoye protivodeystviye ugrozam terrorizma, 2005, No 4, pp. 176-178.
6. Borodakiy Yu.V., Lobodinskiy Yu.G. Informatsionnyye tekhnologii v voyennom dele (osnovy teorii i prakticheskogo primeneniya). M.: Goryachaya liniya - Telekom, 2008. 392 p.
7. Bezkorovaynyy M.M., Tatuzov A.L. Kiberbezopasnost - podkhody k opredeleniyu ponyatiya, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 22-27.
8. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 10-16.
9. Makarenko S.I., Chuklyayev I.I. Terminologicheskiy bazis v oblasti informatsionnogo protivoborstva, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 13-21.
10. Sosnin Yu.V., Kulikov G.V., Nepomnyashchikh A.V., Nashchekin P.A. Bazovyye tekhnologii modelirovaniya protsedur zashchity informatsii ot nesanktsionirovannogo dostupa, Voprosy zashchity informatsii, 2014, No 1 (104), pp. 23-28.





# НЕМОНОТОННЫЕ МОДЕЛИ ОЦЕНКИ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА РАННИХ ЭТАПАХ ИСПЫТАНИЙ

**Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP

Рассмотрены вопросы использования моделей роста надежности в рамках испытаний модифицируемых систем. Обоснованы немонотонные модели оценки надежности программ по результатам обновлений и исправлений. Получены оригинальные расчетные выражения параметров немонотонных моделей оценки надежности, оценки точности и планирования испытаний. Отмечено преимущество немонотонных моделей оценки надежности для программ с открытым кодом и для многоверсионного программного обеспечения.

**Ключевые слова:** надежность программ, технологическая безопасность программ, испытания программ, модели отладки, модели роста надежности, модели оценки надежности, немонотонные модели.

## NONMONOTONE MODELS OF RELIABILITY AND SECURITY OF SOFTWARE IN THE EARLY STAGES OF TESTING

**Alexey Markov**, Ph.D., Associate Professor, CISSP

The use of reliability growth models of the modified systems in the testing phase is examined. The non-monotonic software reliability models on results updates and patches are substantiated. The original expressions of parameters of non-monotonic reliability assessment models, estimates of accuracy and test planning are obtained. The advantages of the non-monotonic reliability growth models for open source software and multi-version software are noted.

**Keywords:** software reliability, software security, software testing, debugging model, reliability growth models, software reliability models, non-monotonic model.

### Введение

На этапах предварительных испытаний и опытной эксплуатации информационных систем важным пунктом является определение момента, когда испытания могут считаться завершёнными<sup>1</sup>. Что касается программных средств (ПС) высокого уровня доверия (например, предназначенных для обработки и защиты гостайны), то современные нормативные документы определяют необходимость формализации результатов испытаний<sup>2</sup>. В таких случаях, к критериям завершения испытаний (которые фиксируются в протоколах испытаний), кроме собственно факта подтверждения вы-

полнения заданных требований, также добавляют значения показателей полноты тестирования и показателей достигнутой степени надежности или корректности с учетом заданной точности оценки.

Для этих целей можно использовать математические модели [1, 3-5, 7-20], которые целесообразно разделить на четыре класса, а именно:

- отладочные модели, позволяющие оценить показатели надежности ПС в зависимости от результатов запусков программ на заданных областях данных и последующих модификаций программ;
- временные модели роста надежности, позволяющие оценить показатели надежности программ в зависимости от времени испытаний с учетом исправлений ошибок программ;
- модели полноты тестирования, позволяющие получить оценки показателей доверия к процессу испытаний;

1 ГОСТ 34.603-92.

2 ГОСТ ИСО/МЭК 15408-3-2013.



- модели сложности программ, основанные на связи метрик сложности ПС с показателями качества, надежности и безопасности программ.

На ранних этапах испытаний, в связи с интенсивной модификацией систем с целью исправления выявляемых ошибок, наиболее адекватными считаются отладочные модели, также называемые моделями роста надежности, основанными на областях входных данных и доработках [17-20]. Известные в литературе модели отражают монотонный рост надёжности функционирования ПС, что не всегда соответствует действительности, например, для случая внедрения программного обеспечения с открытым кодом, многоверсионных или многотиражируемых ПС, когда в процессе их создания в разное время задействованы совершенно различные группы программистов и т.д. Обоснованию немонотонных моделей и получению расчетных выражений их параметров посвящена данная статья.

### Надежность программного обеспечения

Под надежностью программ обычно понимают совокупность свойств, характеризующих способность программы сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени<sup>3</sup>. Если в качестве ограничения уровня пригодности рассматривать дефекты безопасности и уязвимости, то понятие надежности эквивалентно понятию **технологической безопасности**.

Напомним, что определение надежности ПС имеет принципиальное отличие от надежности аппаратных средств, что проявляется, главным образом, в отсутствии эффекта старения ПС во времени. Можно отметить два свойства надежности ПС:

1. Надежность как свойство может изменяться лишь при модификации ПС (т.е. при изменении объекта испытаний), причем степень надежности может как увеличиваться, так и уменьшаться;

2. Значения показателей надежности ПС действительны при тех классах исходных данных, при которых они рассчитывались.

Как отмечалось, в литературе предлагается ряд отладочных моделей, как-то: модель Нельсона [11] и ее модификации [14], модель Пальчуна [9], модель Lapadula [19] и другие [4, 15, 18, 20], которые отражают ступенчатый монотонный рост надежности, т.е. не учитывают возможность явно-

го снижения степени надежности, например, в результате внесения волновых глобальных ошибок или добавления новых функциональных возможностей. Опыт показал, что применение таких математических моделей приводит либо к получению недостоверных результатов, либо существенно увеличивает длительность процесса оценивания надежности ПС. Поэтому требуется обосновать немонотонную модель надежности ПС, получить расчетные выражения ее параметров, в том числе для оценки ее точности.

### Обоснование модели немонотонного роста надежности

Согласно указанному ранее первому свойству надежности ПС, процесс модификации ПС можно условно представить в виде случайного процесса переходов из одного надежностного состояния в другое. Моментами переходов являются модификации объекта испытаний, представляющие собой любые изменения программы с целью исправления обнаруженных ошибок либо развития программы. Определим основной показатель надежности ПС, как степень надежности программы, под которой будем понимать вероятность безошибочного запуска ее на наборе исходных данных из диапазона, определенного спецификациями. С учетом сказанного, имеем следующую модель изменения надежности ПС:

$$P_u = P_0 + \sum_{j=1}^u \Delta P_j,$$

где:  $P_0$  - начальная степень надежности,  $0 \leq P_0 < 1$ ,  $u$  - число проведенных доработок ПС,  $\Delta P_j$  - приращение степени надежности после  $j$ -ой доработки.

Графически процесс изменения надежности ПС представляется ступенчатой функцией роста надежности (рис.1).

Рассматривая ПС как модифицируемую систему, изменение степени надежности ПС после  $j$ -ой доработки можно представить следующим линейным оператором [2]:

$$\Delta P_j = A_j(1 - P_{j-1}) - B_j P_{j-1},$$

где:  $P_{j-1}$  - вероятность безошибочной работы ПС после  $(j-1)$ -ой доработки;  $(1 - P_{j-1})$  - вероятность обнаружения ошибок ПС после  $(j-1)$ -ой доработки;  $A_j$  - коэффициент «эффективности» доработки, характеризующий уменьшение вероятности ошибки за счет  $j$ -ой доработки;  $B_j$  - коэффициент «негативности» доработки, характеризующий снижение степени надежности за счет  $j$ -ой доработки.

3 ГОСТ 28806-90.

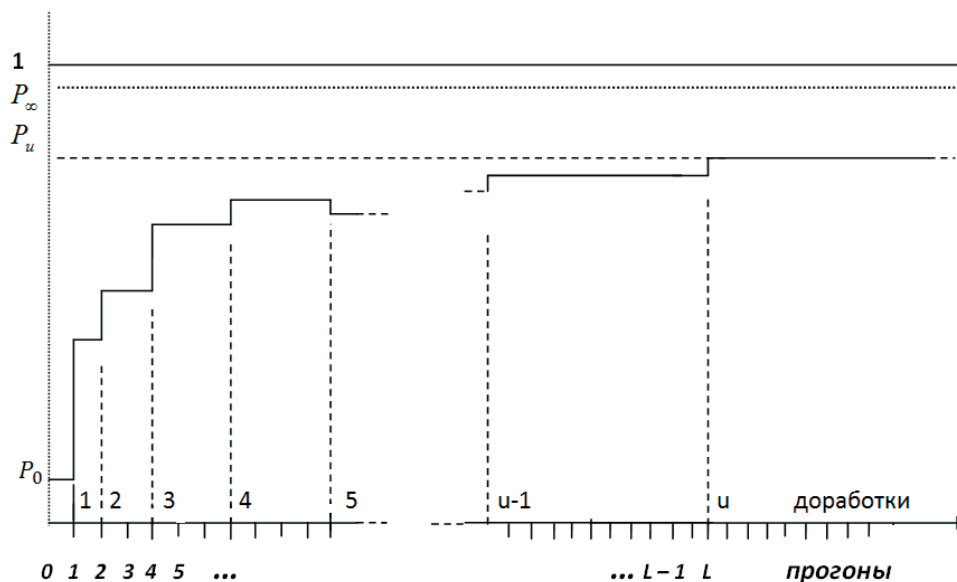


Рис.1. Изменение степени надежности по результатам доработок

Перейдя к рекуррентному выражению и считая предельную степень надежности равной  $P_\infty = \frac{A_j}{A_j + B_j}$ , можно получить модель оценки надежности ПС:

$$P_u = P_\infty - (P_\infty - P_0) \prod_{j=1}^u (1 - A_j / P_\infty), \quad (1)$$

где:  $P_0$  - начальная степень надежности,  $P_\infty$  - предельная степень надежности,  $0 \leq P_0 < P_\infty \leq 1$ ,  $u$  - число проведенных доработок.

Полученное выражение (1) учитывает возможность неравномерного роста степени надежности объекта испытаний и общую тенденцию к снижению роста  $\Delta P_j$  при повышении степени надежности  $P_j$  [2]. Однако в таком представлении модель имеет в целом монотонный вид, так как не учитывается различное влияние принципиально разного рода модификаций, например, изменения ПС с целью исправления ошибок и изменения, связанные с добавлением новых функциональных элементов. Также модель не отражает уровень сложности доработки, а значит возможность внесения волновых ошибок. Иначе говоря, в таком виде модель сводится к классу монотонных моделей роста надежности.

Для исключения данного недостатка предлагается бигеминальная модель оценки надежности, в основе которой лежит использование метрик сложности модификации кода  $k_{ij}$ , например, при исправлении ошибок и при обновлении ПС. На указанную метрику не накладываются ограничения (т.е. метрика сложности может быть любая, наиболее адекватная программной системе и системе программирования<sup>4)</sup>), что обеспечивает полноту описания рассма-

триваемого процесса [7]. Таким образом, полагая  $A_j = \sum_{i=0}^2 a_i k_{ij}$ , можно получить основное расчетное выражение бигеминальной модели оценки надежности:

$$P_u = P_\infty - (P_\infty - P_0) \prod_{j=1}^u (1 - \sum_{i=1}^2 a_i k_{ij} / P_\infty), \quad (2)$$

где:  $u$  - число проведенных доработок,  $a_1$  - коэффициент эффективности доработки ПС с целью исправления ошибки,  $a_2$  - коэффициент эффективности доработки ПС с целью добавления функциональных возможностей,  $k_{ij}$  - объем  $j$ -ой модификации с целью исправления или обновления.

Бигеминальная модель (2) зависит от 4-х параметров ( $P_0, P_\infty, a_1, a_2$ ), расчет которых не представляет труда, например, с помощью метода максимального правдоподобия [8].

Введя классификацию различного рода доработок, в том числе исправляемых ошибок, можно получить обобщенную немонотонную модель оценки надежности:

$$P_u = P_\infty - (P_\infty - P_0) \prod_{j=1}^u (1 - \sum_{i=1}^e a_i k_{ij} / P_\infty), \quad (3)$$

где:  $e$  - число классов модификаций ПС.

Данная модель зависит от  $(e+2)$  параметров. Приведем пример расчета параметров модели.

## Пример расчета параметров модели

Для расчета параметров обобщенной модели (3) можно воспользоваться методом максимального правдоподобия. В качестве исходной статистики можно использовать данные, фиксируемые при испытаниях ПС, а именно: множество испытаний  $\{n_j\}$ , множество неудачных испытаний (отказов)  $\{\hat{m}_j\}$  между доработками, а также множество метрик сложности доработок  $\{k_{ij}\}$ . Тогда при до-

4 IEEE Std. 1061-1998.

пущениях о независимости запусков ПС функция максимального правдоподобия представляет собой вероятность получения общей выборки  $(n_i, \hat{m}_j, j = \overline{1, u})$  числа отказов в проведенных сериях запусков ПС:

$$L_u = \prod_{j=1}^u C_{m_j}^{n_j} P_j^{n_j - \hat{m}_j} (1 - P_j)^{\hat{m}_j},$$

где:  $C_{m_j}^{n_j} = \frac{n_j!}{\hat{m}_j!(n_j - \hat{m}_j)!}$ ,  $u$  - номер последней доработки ПС;  $P_j$  - вероятность успешного исхода каждого из  $n_j$  запусков  $j$ -ой серии;  $\hat{m}_j$  - число отказов в  $n_j$  запусках.

Для удобства можно прологарифмировать и преобразовать функцию  $L_u$  к следующему виду:

$$\ln(L_u) = \sum_{j=1}^u \left( \hat{m}_j \ln(1 - P_\infty + (P_\infty - P_0) \prod_{l=1}^j (1 - \sum_{i=1}^e \frac{a_i k_{ij}}{P_\infty})) + (n_j - \hat{m}_j) \ln(P_\infty + (P_\infty - P_0) \prod_{l=1}^j (1 - \sum_{i=1}^e \frac{a_i k_{ij}}{P_\infty})) \right).$$

Полученная приведенная функция является выпуклой и задана на выпуклом множестве. Поэтому, для нахождения максимума функции правдоподобия можно, например, использовать модифицированный метод наискорейшего спуска с переменным параметром шага  $h^r$ :

$$\begin{cases} P_0^{r+1} = P_0^r + h^r \left( \frac{\partial \ln L(P_0^r, P_\infty^r, a_1^r, \dots, a_e^r)}{\partial P_0} \right); \\ P_\infty^{r+1} = P_\infty^r + h^r \left( \frac{\partial \ln L(P_0^{r+1}, P_\infty^r, a_1^r, \dots, a_e^r)}{\partial P_\infty} \right); \\ a_1^{r+1} = a_1^r + h^r \left( \frac{\partial \ln L(P_0^{r+1}, P_\infty^{r+1}, a_1^r, \dots, a_e^r)}{\partial a_1} \right); \\ \dots \\ a_e^{r+1} = a_e^r + h^r \left( \frac{\partial \ln L(P_0^{r+1}, P_\infty^{r+1}, a_1^{r+1}, \dots, a_e^r)}{\partial a_e} \right), \end{cases}$$

где  $r$  - номер итерации.

Нетрудно показать, что расчетные выражения частных производных приведенной функции максимального правдоподобия имеют следующий вид:

$$\begin{cases} \frac{d \ln L_j}{d P_0} = \sum_{l=0}^j w_l a_l; \\ \frac{d \ln L_j}{d P_\infty} = \sum_{l=0}^j \left( w_l \left( \left( \frac{P_0 - P_\infty}{P_\infty} \alpha_l \beta_l - \alpha_l \right) + 1 \right) \right); \\ \frac{d \ln L_j}{d a_i} = \sum_{l=0}^j \left( w_l \left( \frac{P_0 - P_\infty}{P_\infty} \alpha_l \gamma_{li} \right) \right), \end{cases}$$

$$\text{где } w_j = \frac{n_j - m_j}{P_j} - \frac{m_j}{1 - P_j}; \quad \alpha_j = \prod_{l=1}^j \left( 1 - \frac{\sum_{i=1}^e a_i k_{li}}{P_\infty} \right)$$

$$\beta_j = \sum_{l=1}^j \frac{\sum_{i=1}^e a_i k_{li}}{1 - \sum_{i=1}^e a_i k_{li}/P_\infty}; \quad \gamma_{ji} = \sum_{l=1}^j \frac{-k_{li}}{1 - \sum_{i=1}^e a_i k_{li}/P_\infty}.$$

Для определения оценок  $P_0, P_\infty, a_1, \dots, a_e$ , как показала практика, достаточна следующая точность:

$$\begin{cases} P_0^{r+1} - P_0^r \leq 0.001; \\ P_\infty^{r+1} - P_\infty^r \leq 0.001; \\ a_i^{r+1} - a_i^r \leq 0.0001. \end{cases}$$

Повышенная точность определения параметров  $a_i$  ( $i = \overline{1, e}$ ) связана с их сильным влиянием на функцию  $P_j$  оценки надежности.

Нулевые приближения можно найти методом статистического моделирования на логически рассчитанных интервалах:

$$\begin{cases} 0 \leq P_0 \leq 1 - \left( \frac{M_0}{N_0} \right); \\ 1 - \left( \frac{M_\infty}{N_\infty} \right) \leq P_\infty \leq 1; \\ \frac{1}{K_i e} \left( 1 - \sqrt{\frac{M_\infty N_0}{N_\infty M_0}} \right) \leq a_i \leq \frac{1}{K_i^{max} e}, \end{cases}$$

где:  $M_0$  - число отказов в первых  $N_0$  запусках;  $M_\infty$  - число отказов в последних  $N_\infty$  запусках;  $K_i^{max}$  - максимальное значение  $k_{ij}$  при  $j = \overline{1, u}$ ;  $K_i = \sum_{j=1}^e k_{ji}$ .

Таким образом, полагая, что  $\hat{P}_0, \hat{P}_\infty, \hat{a}_1, \dots, \hat{a}_e$ , случайные величины, равномерно распределенные на указанных ранее интервалах, необходимо проделать определенное число проб и выбрать совокупность параметров, соответствующих максимальной функции правдоподобия. Эта совокупность принимается за искомые начальные значения.

Опыт показал, что на начальных этапах испытаний может возникнуть ситуация, когда не выполняется общая тенденция роста степени надежности ПС при доработках. Это может привести к неточности результатов, получаемых с помощью метода максимального правдоподобия (для расчета максимума функции потребуется бесконечное число итераций).

Для исключения данного недостатка целесообразно использовать метод минимизации относительной энтропии [7]:

$$I_u = \sum_{j=1}^u \left( \frac{m_j}{n_j} \ln \frac{m_j}{n_j P_j} + \frac{n_j - m_j}{n_j} \ln \frac{n_j - m_j}{n_j (1 - P_j)} \right),$$

где:  $m_j$  - число неудачных запусков из общего числа  $n_j$  запусков  $j$ -серии;  $u$  - число проведенных доработок ПС.

Для проверки необходимого и достаточного условия допустимости метода максимального правдоподобия можно воспользоваться следующим соотношением:

$$\frac{\sum_{j=1}^u (j-1)(n_j - m_j)}{\sum_{j=1}^u (j-1)} > \frac{\sum_{j=1}^u (n_j - m_j)}{u}.$$

## Оценка точности модели оценки надежности

Следует сказать, что подавляющее большинство моделей роста надежности представляются авторами без аналитической оценки их точности, что затрудняет их выбор. Данная работа исключает этот недостаток.

Точность оценивания степени надежности ПС можно характеризовать средним квадратическим отклонением. Для получения модели оценки точности удобно воспользоваться методом линеаризации [6]. Тогда среднее квадратическое отклонение находится по следующей формуле:

$$\begin{aligned} \sigma_j = & ((\partial P_j / \partial P_0)^2 \delta_{P_0}^2 + \dots + (\partial P_j / \partial a_e)^2 \delta_{a_e}^2 + \\ & + 2 \left( \frac{\partial P_j}{\partial P_0} \right) \left( \frac{\partial P_j}{\partial P_\infty} \right) \delta_{P_0} \delta_{P_\infty} \rho_{P_0 P_\infty} + \dots + 2 \left( \frac{\partial P_j}{\partial a_{e-1}} \right) \left( \frac{\partial P_j}{\partial a_e} \right) \\ & \delta_{a_{e-1}} \delta_{a_e} \rho_{a_{e-1} a_e} )^{\frac{1}{2}}, \end{aligned}$$

где:  $\rho_{xy}$  - коэффициент корреляции параметров  $x$  и  $y$ .

Для получения значений частных производных функции роста надежности легко найти следующие расчетные выражения:

$$\begin{cases} \frac{dP_j}{dP_0} = \alpha_j; \\ \frac{dP_v}{dP_\infty} = \left( \frac{P_0 - P_\infty}{P_\infty^2} \alpha_j \beta_j - \alpha_j + 1 \right); \\ \frac{dP_j}{da_i} = \frac{P_0 - P_\infty}{P_\infty} \alpha_j \gamma_{ji}, \end{cases}$$

$$\begin{aligned} \text{где: } \alpha_j = & \prod_{l=1}^j \left( 1 - \frac{\sum_{i=1}^e a_i k_{li}}{P_\infty} \right), \beta_j = \sum_{l=1}^j \frac{\sum_{i=1}^e a_i k_{li}}{1 - \sum_{i=1}^e a_i k_{li} / P_\infty}, \\ \gamma_{ji} = & \sum_{l=1}^j \frac{-k_{li}}{1 - \sum_{i=1}^e a_i k_{li} / P_\infty}. \end{aligned}$$

Остальные параметры формулы можно получить из ковариационной матрицы, содержащей дисперсии и корреляционные моменты искомых оценок:

$$\mathcal{K} = \begin{bmatrix} \delta_{P_0}^2 & \delta_{P_0} \delta_{P_\infty} \rho_{P_0 P_\infty} & \dots & \delta_{P_0} \delta_{a_e} \rho_{P_0 a_e} \\ \delta_{P_0} \delta_{P_\infty} \rho_{P_0 P_\infty} & \delta_{P_\infty}^2 & \dots & \delta_{P_\infty} \delta_{a_e} \rho_{P_\infty a_e} \\ \dots & \dots & \dots & \dots \\ \delta_{P_0} \delta_{a_e} \rho_{P_0 a_e} & \delta_{P_\infty} \delta_{a_e} \rho_{P_\infty a_e} & \dots & \delta_{a_e}^2 \end{bmatrix}$$

Для ее построения можно воспользоваться следующим соотношением:

$$\mathcal{K} = -\mathcal{M}^{-1},$$

где:  $\mathcal{M}$  - матрица вторых частных производных функции правдоподобия:

$$\mathcal{M} = \begin{bmatrix} \frac{\partial^2 \ln L_u}{\partial P_0^2} & \frac{\partial^2 \ln L_u}{\partial P_0 P_\infty} & \dots & \frac{\partial^2 \ln L_u}{\partial P_0 a_e} \\ \dots & \dots & \dots & \dots \\ \frac{\partial^2 \ln L_u}{\partial P_\infty P_0} & \frac{\partial^2 \ln L_u}{\partial P_\infty^2} & \dots & \frac{\partial^2 \ln L_u}{\partial P_\infty a_e} \\ \dots & \dots & \dots & \dots \\ \frac{\partial^2 \ln L_u}{\partial P_0 a_e} & \frac{\partial^2 \ln L_u}{\partial P_\infty a_e} & \dots & \frac{\partial^2 \ln L_u}{\partial a_e^2} \end{bmatrix}.$$

Для расчета вторых частных производных легко получить следующие расчетные выражения:

$$\begin{cases} \frac{d \ln L_u}{d P_0} = \sum_{j=0}^u w_j a_j; \\ \frac{d \ln L_u}{d P_\infty} = \sum_{j=1}^u \left( w_j \left( \left( \frac{P_0 - P_\infty}{P_\infty} \alpha_j \beta_j - \alpha_j \right) + 1 \right) \right); \\ \frac{d \ln L_u}{d a_i} = \sum_{j=0}^u \left( w_j \left( \frac{P_0 - P_\infty}{P_\infty} \alpha_j \gamma_{ji} \right) \right), \end{cases}$$

$$\text{где: } w_j = \frac{n_j - m_j}{P_j} - \frac{m_j}{1 - P_j}.$$

## Планирование испытаний

В процессе управления надежностью ПС следует решать задачи планирования затрат на тестирование и испытания для достижения требуемого уровня надежности ПС. В таком случае полезно оценить тенденции по процессу развития и внедрения программного продукта, получить прогноз числа оставшихся ошибок и сложности их исправления.

Для расчета ряда показателей планирования можно воспользоваться моделями (1-3). К сожалению, статистические модели оценки надежности не позволяют спрогнозировать частоту исправлений конкретного типа, а лишь используют эту информацию. Проведение доработок конкретного типа зависит от условий эксплуатации, достигнутой степени надежности, требований по надежности к ПС, квалификации и опыта разработчиков и, следовательно, их содержание может меняться. Для учета типов доработок целесообразно воспользоваться теорией многофакторного анализа. Поскольку изменение числа исправлений конкретного типа рассматривается в масштабе проведения доработок, то для аппроксимации функции сложности модификации ПС можно использовать, например, многочлен второй степени от одной переменной:

$$k_j = \kappa_0 + \kappa_1 j + \kappa_2 j^2,$$

где:  $\kappa_0, \kappa_1, \kappa_2$  - параметры многочлена;  $j = \overline{1, u}$ .



Легко показать, что параметры многочлена имеют следующий вид:

$$\left\{ \begin{array}{l} \kappa_0 = \frac{30(\sum_{j=1}^u \hat{k}_j - \frac{2}{u(u-1)} \sum_{j=1}^u \hat{k}_j j^2 - \beta_2(2 + 3u - 3u^2 - 2u^3))}{10(u-1)}; \\ \kappa_1 = \frac{6(\sum_{j=1}^u \hat{k}_j - \frac{2}{u+1} \sum_{j=1}^u \hat{k}_j j - \beta_2(1 - u^2)u)}{u(1-u)}; \\ \kappa_2 = \frac{\sum_{j=1}^u \hat{k}_j \frac{u^2 + 3u - 2}{2} - u \sum_{j=1}^u \hat{k}_j j - \frac{2}{u-1} \sum_{j=1}^u \hat{k}_j j^2}{u - (4 - u^2)}. \end{array} \right.$$

Тогда, считая, что по имеющимся данным об испытаниях получены оценки параметров модели и достигнутой степени надежности ПС  $P_u$ , имеем следующее расчетное выражение модели прогноза степени надежности:

$$P_{\text{тр}} = P_{\infty} - (P_{\infty} - P_u) \prod_{i=u+1}^{u+j} (1 - \sum_{i=1}^e a_i k_{ij} / P_{\infty}), \quad (4)$$

где:  $P_{\text{тр}}$  - требуемая степень надежности ПС;  $u$  - номер последней проведенной доработки;  $j$  - число планируемых доработок.

Расчет необходимого числа доработок для достижения требуемой степени надежности можно выполнить путем циклического пересчета выражения (4). Для этого рассчитывается значение  $P_u$  по формуле (4) и далее в цикле, увеличивая  $j$ , определяем значение  $P_{u+j}$ . При выполнении условия  $P_{u+j} \geq P_{\text{тр}}$  осуществляется выход из цикла.

Для простоты использования прогнозирующей модели положим  $A_j = a$ , что соответствует переходу от модели (3) к (1). Тогда, упростив выражение (4) и прологарифмировав его, получим следующее выражение для оценки числа  $J$  необходимых доработок ПС для достижения требуемой степени надежности  $P_{\text{тр}}$ :

$$J = \left\lceil \left\| \frac{\ln(\frac{P_{\infty} - P_{\text{тр}}}{P_{\infty} - P_u})}{\ln(1 - a/P_{\infty})} \right\| \right\rceil,$$

где:  $\lceil \mathbb{X} \rceil$  - операция получения ближайшего наибольшего целого  $\mathbb{X}$ ,  $a$  - усредненный коэффициент эффективности доработки ПС.

Считая, что при доработках не вносятся дополнительные ошибки (т.е.  $P_{\infty} = 1$ ), можно получить формулу числа оставшихся ошибок после  $u$ -ой доработки:

$$N_u = \left\lceil \left\| \frac{\ln(\frac{1 - P_{\text{тр}}}{1 - P_u})}{\ln(1 - a)} \right\| \right\rceil.$$

## Апробация немонотонной модели оценки надежности

В результате исследований установлено, что предложенные немонотонные модели (2) и (3) обладают высокой точностью ( $\sigma_j < 0.001$ ) при числе доработок более 10 и числе запусков более 50. Для контроля согласованности модели с исходными данными использовался критерий Мизеса (при пороговом значении 0.01) [6].

Исследование влияния коэффициента эффективности доработок ПС на точность результатов модели (3) показало, что при учете категорирования доработок точность может повышаться на порядок.

Сравнительный анализ предложенных моделей с известными отладочными моделями показал ряд их преимуществ, а именно:

- учет возможного резкого снижения степени надежности при обновлениях;
- возможность учета сложности доработок;
- отсутствие ограничений на организацию испытаний и сбора информации;
- возможность учета показателей надежности ПС, полученных на предыдущих этапах разработки и внедрения;
- отсутствие субъективных параметров, как-то: квалификация программиста и уровень технологии программирования;
- простота использования - нет необходимости рассчитывать вероятности реализации всех путей программы, как, например, в модели Нельсона и её модификациях [11, 14].

## Выводы

В работе, фактически, обоснован метод планирования испытаний, основанный на использовании обобщенной немонотонной модели оценки надежности ПС по результатам запусков и модификаций. В рамках предложенного метода получены

расчетные выражения параметров модели оценки надежности ПС, а также оценки точности и планирования испытаний. Предложенная обобщенная немонотонная модель (3) позволяет учесть возможные моменты снижения степени надежности ПС, что свойственно, например, разработке программ с открытым кодом, многоверсионных программ и др. Точность обобщенной модели зависит от решения задачи классификации доработок ПС. Модель может быть интегрирована с показателями надежности функционирования ПС, полученными на ранних стадиях разработки программ. Упрощение модели позволяет свести ее к экспоненциальным NHPP-моделям роста надежности, используемым на этапах эксплуатации и совершенствования информационных систем [8].

Основным достоинством предложенных немонотонных моделей является возможность повышения точности (за счет категорирования модификаций) более чем на 10%, что равноценно снижению на 5-15% необходимого числа запусков ПС в процессе испытаний.

Следует отметить, что к недостаткам отладочных моделей относят их низкую точность при малой статистике, что, однако, можно избежать путем применения соответствующих приемов повышения точности, в том числе метода Вальда [10].

Предложенный метод и модели могут быть рекомендованы также для оценки показателей разного рода модифицируемых и обучающихся систем.

### Литература

1. Александрович А.Е., Бородакий Ю.В., Чуканов В.О. Проектирование высоконадёжных информационно-вычислительных систем. М.: Радио и связь, 2004. 144 с.
2. Волков Л.И. Управление эксплуатацией летательных комплексов. М.: Высшая школа, 1981. 226 с.
3. Гуров Д.В., Гуров В.В., Иванов М.А. Использование моделей надежности программного обеспечения для оценки защищенности программного комплекса // Безопасность информационных технологий. 2012. № 1. С. 88-91.
4. Карповский Е.Я., Чижов С.А. Надежность программной продукции. Киев: Техника, 1990. 160 с.
5. Королев В.Ю. Некоторые критерии проверки надежности программного обеспечения // Системы и средства информатики. 2013. Т. 23. № 1. С. 132-142.
6. Ллойд Д., Липов М. Надежность. М.: Сов.радио, 1964. 668 с.
7. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации. Вестник МГТУ им. Н.Э.Баумана. Сер. «Приборостроение». 2011. Спецвыпуск. С.90-103.
8. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов; под ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.
9. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. СПб.: Наука, 1994. 84 с.
10. Смагин В.А. Основы теории надежности программного обеспечения. - СПб.: ВКА им. А.Ф.Можайского, 2009. 336 с.
11. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения: Анализ крупномасштабных разработок: Пер. с англ. М.: Мир, 1981. 323 с.

### Reference

1. Aleksandrovich A.E., Borodakiy Yu.V., Chukanov V.O. Proyektirovaniye vysokonadezhnykh informatsionno-vychislitelnykh system. Moscow, Radio i svyaz, 2004. 144 p.
2. Volkov L.I. Upravleniye ekspluatatsiyey letatelnykh kompleksov, Moscow, Vysshaya shkola, 1981, 226 p.
3. Gurov D.V., Gurov V.V., Ivanov M.A. Ispolzovaniye modeley nadezhnosti programmnogo obespecheniya dlya otsenki zashchishchennosti programmnogo kompleksa, Bezopasnost informatsionnykh tekhnologiy, 2012, No 1, pp. 88-91.
4. Karpovskiy Ye.Ya., Chizhov S.A. Nadezhnost programmnoy produktsii, Kiyev: Tekhnika, 1990, 160 p.
5. Korolev V.Yu. Nekotoryye kriterii proverki nadezhnosti programmnogo obespecheniya, Sistemy i sredstva informatiki, 2013, Vol. 23, No 1, pp. 132-142.
6. Lloyd D., Lipow M. Nadezhnost. M.: Sov.radio, 1964. 668 p.
7. Markov A.S. Modeli otsenki i planirovaniya ispytaniy programnykh sredstv po trebovaniyam bezopasnosti informatsii. Vestnik MGTU im. N.E.Baumana. Ser. «Priborostroyeniye», 2011, Spetsvypusk, pp.90-103.
8. Markov A.S., Tsirllov V.L., Barabanov A.V., Metody otsenki nesootvetstviya sredstv zashchity informatsii, by ed. A.S.Markov, Moscow, Radio i svyaz, 2012, 192 p.
9. Palchun B.P., Yusupov P.M. Otsenka nadezhnosti programmnogo obespecheniya. Saint Petersburg, Nauka, 1994, 84 p.
10. Smagin V.A. Osnovy teorii nadezhnosti programmnogo obespecheniya, Saint Petersburg, VKA im. A.F.Mozhayskogo, 2009, 336 p.
11. Teyer T., Lipow M., Nelson E. Nadezhnost programmnogo obespecheniya: Analiz krupnomasshtabnykh razrabotok, Moscow, Mir, 1981, 323 p.



12. Титов А.В., Харьковской А.А., Чуканов В.О. Модели надежности программного обеспечения ответственного назначения // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление, 2011. Т. 2. № 120. С. 123-126.
13. Царевский А.В. Обеспечение надежности аппаратно-программных комплексов обмена информацией // Автоматизация процессов управления. 2011. №2. С. 56-65.
14. Черкесов Г. Н. Надежность аппаратно-программных комплексов. СПб.: «Питер», 2005. 479 с.
15. Штрик А.А., Осовецкий Л.Г., Мессих И.Г. Структурное проектирование надежных программ встроенных ЭВМ. Л.: Машиностроение, 1989. 296 с.
16. Шубинский И.Б., Замышляев А.М., Прошин Г.Б. Функциональная надежность программного обеспечения информационных систем // Надежность. 2011. Т. 38. № 3. С. 72-81.
17. Musa J.D. More Reliable Software Faster and Cheaper. 2nd Edition. TATA McGraw-Hill, 2004. 632 p.
18. Pham H. System Software Reliability. Springer Series in Reliability Engineering. Springer, 2006. 440 p.
19. Shanmugam L., Florence L. An Overview of Software Reliability Models // International Journal of Advanced Research in Computer Science and Software Engineering. 2012. Vol. 2. № 10. P. 36-42.
20. Xie M., Dai Y.-S., Poh K.-L. Computing Systems Reliability. Models and Analysis. Kluwer, 2004. 293 p.
12. Titov A.V., Kharkovoy A.A., Chukanov V.O. Modeli nadezhnosti programmogo obespecheniya otvetstvennogo naznacheniya, Nauchno-tehnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravleniye, 2011, Vol. 2, No 120, pp. 123-126.
13. Tsarevskiy A.V. Obespecheniye nadezhnosti apparatno-programmnykh kompleksov obmena informatsiyey, Avtomatizatsiya protsessov upravleniya, 2011, No 2, pp. 56-65.
14. Cherkesov G. N. Nadezhnost apparatno-programmnykh kompleksov. Saint Petersburg, Piter, 2005, 479 p.
15. Shtrik A.A., Osovetskiy L.G., Messikh I.G. Strukturnoye proyektirovaniye nadezhnykh programm vstroyennykh EVM. Leningrad, Mashinostroyeniye, 1989, 296 p.
16. Shubinskiy I.B., Zamyshlyayev A.M., Proshin G.B. Funktsionalnaya nadezhnost programmogo obespecheniya informatsionnykh sistem, Nadezhnost, 2011, Vol. 38, No 3, pp. 72-81.
17. Musa J.D. More Reliable Software Faster and Cheaper. 2nd Edition. TATA McGraw-Hill, 2004. 632 p.
18. Pham H. System Software Reliability. Springer Series in Reliability Engineering. Springer, 2006. 440 p.
19. Shanmugam L., Florence L. An Overview of Software Reliability Models, International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol. 2, No 10, pp. 36-42.
20. Xie M., Dai Y.-S., Poh K.-L. Computing Systems Reliability. Models and Analysis. Kluwer, 2004, 293 p.



# ВЛИЯНИЕ ВРЕМЕНИ ВОССТАНОВЛЕНИЯ СИНХРОНИЗАЦИИ НА ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ ИНФОТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

*Парамонов Иван Юрьевич, кандидат технических наук*

В статье рассматривается проблема нормирования требований устойчивости инфотелекоммуникационных сетей. Обосновывается необходимость учета влияния времени восстановления синхронизации на показатели надежности и живучести. Показано влияние времени восстановления синхронизации после воздействия дестабилизирующих факторов на показатели надежности и живучести сетей.

**Ключевые слова:** инфотелекоммуникационные сети, устойчивость, надежность, живучесть, синхронизация, дестабилизирующие факторы

## THE INFLUENCE OF RECOVERY TIME SYNCHRONIZATION ON THE SUSTAINABILITY PERFORMANCE OF INFOTELECOMMUNICATION NETWORKS

*Ivan Paramonov, Ph.D.*

Article considers the problem of rationing requirement for the sustainability infotelecommunication networks. The need to consider the effect of time of restoration of synchronization on reliability and survivability substantiates. Influence on indicators of reliability and survivability of networks of time of restoration of synchronization after influence of destabilizing factors is shown.

**Keywords:** infotelecommunication network, sustainability, reliability, survivability, synchronization, destabilizing factors

### Введение

Развитие инфотелекоммуникационных сетей (ИТКС) привели к повышению требований к нормированию характеристик средств, комплексов и систем связи. В частности, одним из основных требований к оборудованию ИТКС является обеспечение возможности достоверной оценки характеристик оборудования на различных стадиях жизненного цикла.

Отсутствие данных о свойствах оборудования или их недостаточно достоверные оценки полностью или в значительной степени обесценивают информацию об эффективности функционирования ИТКС.

Для современных ИТКС характерно усложнение условий функционирования. Это связано с расширением сфер использования телекоммуникационных технологий, увеличением количества радиоэлектронных средств, повышением «ценности» информации, появлением новых источников угроз нарушения безопасности ИТКС и т. д.

Важным свойством оборудования ИТКС, влияющим на эффективность функциониро-

вания, является его устойчивость. Оценка устойчивости ИТКС и их элементов должна быть максимально близкой «оценкой сверху» к реальным значениям, а набор показателей устойчивости должен обеспечивать получение гарантированных оценок на всех стадиях жизненного цикла. Некорректная оценка характеристик устойчивости ИТКС чревата экономическими потерями, техническими последствиями, что может влиять на эффективность функционирования как ИТКС, так и критически важных объектов, в составе которых они используются.

### 1. Анализ требований к показателям устойчивости

Под устойчивостью понимается способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов<sup>1</sup>.

<sup>1</sup> ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. стр. 2 п.3.3

Устойчивость оборудования ИТКС определяется:

- свойствами оборудования;
- способами применения;
- правильностью настройки;
- условиями эксплуатации;
- значениями характеристик, внутренних и внешних дестабилизирующих факторов и т. д.

Оценивание устойчивости ИТКС является сложной и комплексной задачей, т.к. требует учета большого количества факторов в условиях неопределенности как о количестве влияющих факторов, так и о значениях их параметров.

При проектировании и выборе оборудования связи необходимо учитывать характеристики устойчивости в нормальных и рабочих условиях эксплуатации, т.е. в условиях воздействия влияющих (учитываемых) внутренних и внешних дестабилизирующих факторов (ДФ).

Данные об устойчивости оборудования должны приводиться в нормативно-технической документации на оборудование. При отсутствии таких данных или их недостаточности необходимо проводить экспериментальное их определение (доопределение), что должно быть исключительным случаем и применяться редко. При создании систем и комплексов связи значения характеристик устойчивости необходимо получать расчётным и подтверждать экспериментальным путем, или, как исключение, экспериментальным путём.

Номенклатура и способ представления характеристик устойчивости должны соответствовать задачам, стоящим как перед разработчиками, так и перед потребителями.

Таким важным требованием к номенклатуре показателей устойчивости является обеспечение возможности контроля характеристик устойчивости оборудования на практике.

С учётом условий и особенностей применения оборудования связи характеристики устойчивости нормируются для следующих условий эксплуатации:

- а) нормальные условия;
- б) рабочие условия.

Нормирование характеристик устойчивости в рабочих условиях при воздействии ДФ необходимо

проводить с учётом динамических характеристик как оборудования, так и оговоренных в задании ДФ [1]<sup>2</sup>.

## 2. Учёт влияния параметров дестабилизирующих факторов на устойчивость

В соответствии с [1] в качестве показателя устойчивости оборудования связи используется коэффициент готовности  $K_r$  и коэффициент оперативной готовности  $K_{ог}$ :

$$K_r = T_0 / (T_0 + T_B); \quad (1)$$

$$K_{ог} = P(T) K_r, \quad (2)$$

где  $T_0$  – среднее время наработки на отказ;  $T_B$  – среднее время восстановления работоспособности;  $P(T)$  – вероятность сохранения работоспособности при воздействии ДФ.

Коэффициент готовности  $K_r$  характеризует надёжность, а коэффициент оперативной готовности  $K_{ог}$  – живучесть оборудования связи.

Если  $T_B$  представить как совокупность отдельных интервалов воздействия ДФ, то выражения (1), (2) примут вид:

$$K_r = T_0 / (T_0 + NT_i); \quad (3)$$

$$K_{ог} = P(T) T_0 / (T_0 + NT_i), \quad (4)$$

где  $N$  – число случаев воздействия ДФ;  $T_i$  – средняя длительность воздействия ДФ.

В качестве критерия отказа при передаче данных принимается повышение отношения числа битов, принятых с ошибками, к общему числу принятых битов до  $10^{-3}$  в течение 10 последовательных секунд и больше<sup>3</sup>.

Результаты расчёта показателей устойчивости в соответствии с критериями, приведёнными в [1], приведены в таблицах 1, 2 и на рисунках 1, 2. Результаты получены без учета времени, которое необходимо ИТКС для восстановления и возобновления обслуживания.

<sup>2</sup> Рекомендация МСЭ-R.S.1522-1 Воздействие потери времени восстановления синхронизации на готовность в гипотетических эталонных цифровых трактах: [Электронный ресурс]. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-I!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-I!!PDF-R.pdf).

<sup>3</sup> ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. стр. 7 п.5.38

Таблица 1 – Зависимость  $K_r$  от числа и длительности воздействия ДФ

$K_r$	$T_B, c$	$T_i, c$			
		$N$			
		10	100	1000	10000
0,99	318545,4545	31854,55	3185,455	318,5455	31,85455
0,999	31567,56757	3156,757	315,6757	31,56757	3,156757
0,9999	3153,915392	315,3915	31,53915	3,153915	0,315392

Таблица 2 – Зависимость  $K_{ог}$  от числа и длительности воздействия ДФ

$K_r$	$P$	$T_i, c$	$K_{ог}$			
			$N$			
			10	100	1000	10000
0,99	0,8	10	0,80000	0,799975	0,799746	0,797471
		100	0,79997	0,799746	0,797471	0,775412
		1000	0,79975	0,797471	0,775412	0,607396
0,999	0,85	10	0,85000	0,849973	0,849731	0,847313
		100	0,84997	0,849731	0,847313	0,823875
		1000	0,84973	0,847313	0,823875	0,645358
0,9999	0,9	10	0,90000	0,899971	0,899715	0,897155
		100	0,89997	0,899715	0,897155	0,872338
		1000	0,89971	0,897155	0,872338	0,68332

В качестве критерия готовности канала связи применяется интервал времени из 10 последовательных секунд, в течение которых вероятность ошибки меньше или равна  $10^{-3}$ .<sup>4</sup>

Однако необходимо различать готовность канала и готовность обслуживания. Готовность обслуживания учитывает также время, необхо-

димое для восстановления синхронизации, т.е. время на повторное вхождение в синхронизм. Время восстановления синхронизации зависит от скорости передачи информации, вида модуляции, используемого помехоустойчивого кода, схемы (алгоритма) демодулятора и декодера и т. д.<sup>5</sup>.

<sup>4</sup> Рекомендация МСЭ-R.S.1522-1 Воздействие потери времени восстановления синхронизации на готовность в гипотетических эталонных цифровых трактах: [Электронный ресурс]. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf). стр. 1 п. г.

<sup>5</sup> Рекомендация МСЭ-R.S.1522-1 Воздействие потери времени восстановления синхронизации на готовность в гипотетических эталонных цифровых трактах: [Электронный ресурс]. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf). стр.4 п. 3.

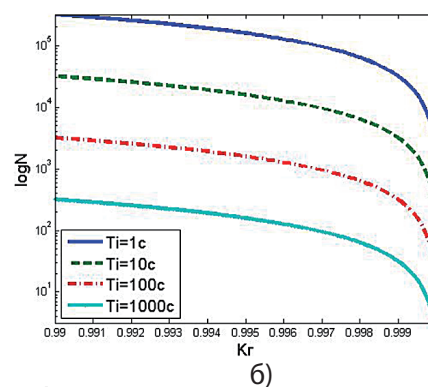
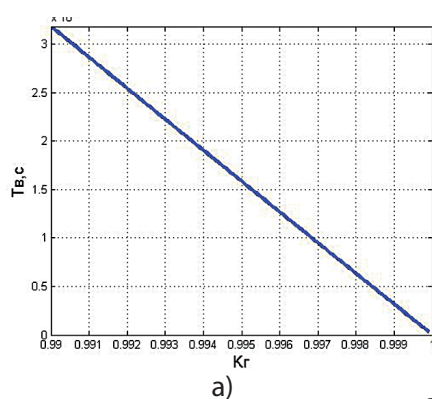


Рисунок 1

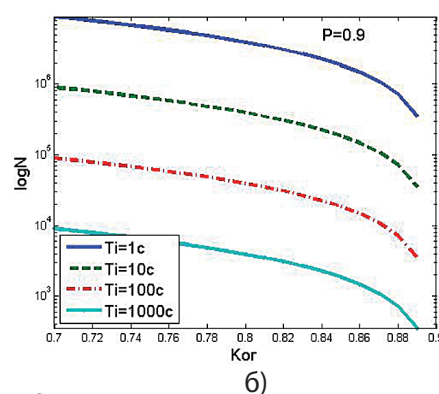
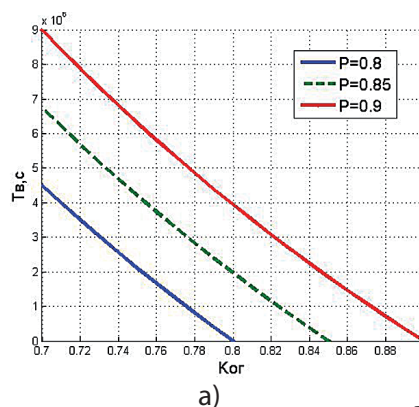


Рисунок 2

## Влияние времени восстановления синхронизации на показатели устойчивости

С учётом времени вхождения в синхронизм выражения (3) и (4) примут вид:

$$K_{ГБ} = T_0 / (T_0 + N(T_i + T_{Bi})); \quad (5)$$

$$K_{ОГБ} = P(T)T_0 / (T_0 + N(T_i + T_{Bi})), \quad (6)$$

где  $T_{Bi}$  – время восстановления (вхождения в синхронизм) после прекращения воздействия ДФ.

В таблице 3 приведены значения максимального времени восстановления обслуживания, по-

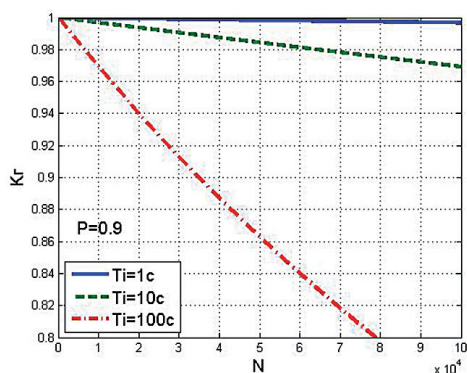
лученные экспериментальным путем<sup>6</sup>.

На рисунках 3, 4 и в таблицах 4 – 6 приведены результаты расчёта  $K_{Г}$  и  $K_{ОГ}$  с учётом времени восстановления.

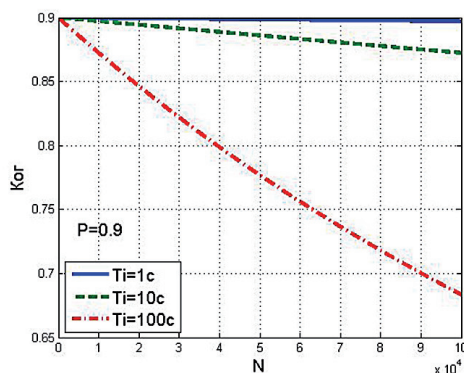
<sup>6</sup> Рекомендация МСЭ-R.S.1522-1 Воздействие потери времени восстановления синхронизации на готовность в гипотетических эталонных цифровых трактах: [Электронный ресурс]. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-1!!PDF-R.pdf). стр. 3 таблица 2.

**Таблица 3 – Максимальное время восстановления обслуживания**

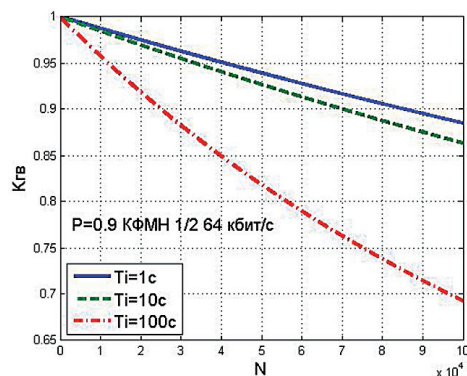
Модуляция и кодирование	Скорость передачи данных на несущей	Время восстановления, с
КФМН 1/2	64 кбит/с	40,0
	2 Мбит/с	4,5
КФМН 3/4	64 кбит/с	19,8
	2 Мбит/с	6,0
	8 Мбит/с	9,3
	34 Мбит/с	2,3
8-ФМН 2/3 РС (201, 219)	2 Мбит/с	3,1
	8 Мбит/с	9,1
	34 Мбит/с	4,0



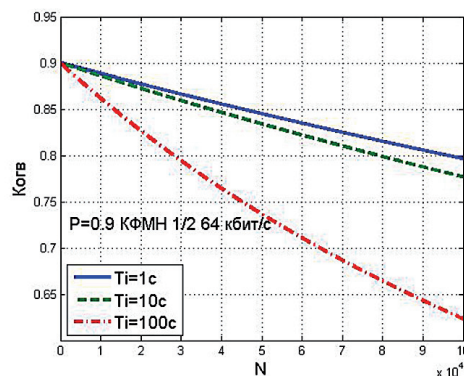
а)



б)



в)



г)

**Рисунок 3**



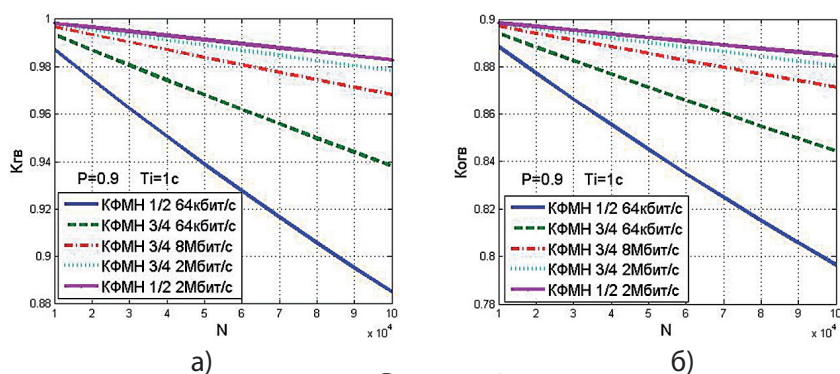


Рисунок 4

Таблица 4 – Зависимость  $K_{ГВ}$  от времени восстановления

Вид модуляции	Скорость передачи информации	Время восстановления, $T_{vi}$ , с	$T_i$ , с	$K_{ГВ}$			
				$N$			
				10	100	1000	10000
КФМН 1/2	64 кбит/с	40	1	0,9999870	0,999870	0,998702	0,987166
			100	0,999956	0,999556	0,995580	0,957493
	2 Мбит/с	4,5	1	0,9999983	0,999983	0,999826	0,998259
			100	0,999967	0,999669	0,996697	0,967926
КФМН 3/4	64 кбит/с	19,8	1	0,9999934	0,999934	0,999341	0,993448
			100	0,999962	0,999620	0,996216	0,963402
	2 Мбит/с	6	1	0,9999978	0,999978	0,999778	0,997785
			100	0,999966	0,999664	0,996650	0,967481
	8 Мбит/с	9,3	1	0,9999967	0,999967	0,999673	0,996745
			100	0,999965	0,999654	0,996546	0,966502

Таблица 5 – Зависимость  $K_{ог}$  от времени восстановления

Вид модуляции	Скорость передачи информации	Время восстановления, $T_{vi}$ , с	$T_i$ , с	$K_{огв}$			
				$N$			
				10	100	1000	10000
$P=0,9$							
КФМН 1/2	64 кбит/с	40	1	0,899988	0,899883	0,899703	0,897042
			100	0,899960	0,899601	0,897144	0,872231
	2 Мбит/с	4,5	1	0,899998	0,899984	0,899713	0,897142
			100	0,899970	0,899702	0,897154	0,872326
КФМН 3/4	64 кбит/с	19,8	1	0,899994	0,899941	0,899709	0,897099
			100	0,899966	0,899658	0,897150	0,872285
	2 Мбит/с	6	1	0,899998	0,899980	0,899713	0,897138
			100	0,899970	0,899698	0,897153	0,872322
	8 Мбит/с	9,3	1	0,899997	0,899971	0,899712	0,897129
			100	0,899969	0,899688	0,897153	0,872313

Таблица 6 – Зависимость  $K_{Г}$  и  $K_{ог}$  от времени восстановления

Вид модуляции, скорость передачи информации	Время восстановления, $T_{\text{в}}; \text{с}$	$K_{\text{Г}}$	$K_{\text{ГВ}}$		$K_{\text{ОГВ}}$ $(P = 0,9)$	$K_{\text{ОГВ}}$	
			$N$				
			1000	10000		1000	10000
КФМН 1/2 64 кбит/с	40	0,99	0,988	0,977	0,891	0,8898	0,8799
КФМН 3/4 34 Мбит/с	2,3		0,9899	0,9892		0,8909	0,8903
КФМН 1/2 64 кбит/с	40	0,9999	0,9986	0,9873	0,8999	0,8987	0,8886
КФМН 3/4 34 Мбит/с	2,3		0,9998	0,9992		0,8998	0,8992



Анализ данных, приведённых на рисунках 1 – 4 и в таблицах 4 – 6 показывает, что необходимо учитывать не только количество и длительности интервалов неготовности канала связи, но и тех интервалов времени, которые необходимы для восстановления системы после прекращения воздействия дестабилизирующих факторов. В ряде случаев большое количество кратковременных воздействий может приводить к большим интервалам неготовности, чем меньшее количество воздействий большей длительности.

### Заключение

Краткий анализ требований к устойчивости ИТКС показал, что существующие подходы к нормированию требований к устойчивости ИТКС требуют корректировки в части учета динамических характеристик ДФ и оборудования связи. Также необходимо нормировать параметры, позволяющие учесть влияния характеристик каналов, трактов и дестабилизирующих факторов на время вхождения в синхронизм.

В настоящее время при нормировании показателей устойчивости ИТКС учитывается только необходимость обеспечения «готовности канала». Приведенные результаты расчетов показали, что для оценивания устойчивости ИТКС необходимо задавать и учитывать требования и к показателям

«готовности обслуживания». При выборе и нормировании показателей устойчивости ИТКС необходимо учитывать как «готовность канала», так и «готовность обслуживания».

Мало изученным, но очень важным вопросам является исследование распределения времени неготовности на коротких временных интервалах: час, сутки и т.д. [1]<sup>7</sup>. Такие исследования особенно важны для ИТКС, которые используются в системах информационного обеспечения функционирования критически важных и потенциально опасных объектов, в том числе транспортной и энергетической инфраструктуры.

В статье сделана попытка на относительно грубом, но достаточно показательном примере привлечь внимание специалистов к проблемным вопросам нормирования требований устойчивости инфотелекоммуникационных систем и сетей. В дальнейшем планируется провести исследования и получить выражения для вычисления показателей устойчивости ИТКС с учетом вероятностных характеристик параметров как дестабилизирующих факторов, так и оборудования связи.

<sup>7</sup> Рекомендация МСЭ-R.S.1522-1 Воздействие потери времени восстановления синхронизации на готовность в гипотетических эталонных цифровых трактах: [Электронный ресурс]. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-I!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1522-1-200502-I!!PDF-R.pdf). стр. 17 п.6

### Литература

1. Информационные технологии в радиотехнических системах: учеб. пособие. – 2-е изд., перераб. и доп. / В.А. Васин, И.Б. Власов, Ю.М. Егоров и др.; под ред. И.Б. Фёдорова. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 768 с.

### References

1. Informacionnye tehnologii v radiotekhnicheskikh sistemah: ucheb. posobie. – 2-e izd., pererab. i dop. / V.A. Vasin, I.B. Vlasov, Ju.M. Egorov i dr.; pod red. I.B. Fjodorova. – M.: Izd-vo MGTU im. N.Je. Bauman, 2004. – 768 s.



# ЭТАЛОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ И ОБОСНОВАНИЕ НА ЕЕ ОСНОВЕ НОВЫХ НАПРАВЛЕНИЙ РАЗВИТИЯ ТЕОРИИ СТЕГАНОГРАФИИ

*Макаренко Сергей Иванович, кандидат технических наук*

*В работе уточняется и дополняется терминологический базис теории стеганографии, а также предлагается обобщение известных методов и способов реализации стеганографических систем связи на основе эталонной модели взаимодействия стеганографических систем. Данная модель формализует описание взаимодействия абонентов стеганографических систем связи на различных функциональных уровнях: уровне системы связи, уровне контейнера, уровне стегоканала, уровне стегосети, уровне стего-транспорта, уровне сообщений. Представлены объекты, предметы и процессы, формализуемые на каждом из уровней. Приводятся перспективные направления развития стеганографических систем связи на основе предложенной модели.*

**Ключевые слова:** стеганография, скрытая передача данных, стеганографическая система.

## THE STEGANOGRAPHIC SYSTEM INTERCONNECTION BASIC REFERENCE MODEL AND THE JUSTIFICATION OF NEW AREAS OF STEGANOGRAPHY THEORY'S DEVELOPMENT

*Sergey Makarenko, Ph.D. in Technical Sciences*

*This article consists of revision terms of steganography theory and suggest the steganographic system interconnection basic reference model (SSI model) for generalization of researched steganography methods and means. This model formalizes the interconnection of steganographic communication systems` users on different function levels: communication level, steganography container level, steganography channel level, steganography network level, steganography transport level and message level. Objects, subjects and process of steganography systems define for every this levels. The perspective areas of development of steganographic communication systems based on SSI model are shown.*

**Keywords:** steganography, undetected data communications, steganographic systems.

Глобальное распространение вычислительных и телекоммуникационных систем привело к необходимости обеспечения безопасности передаваемых данных, доступа к ним, а также защиты авторских прав на различные виды информации, циркулирующей в интернете. В связи с этим, стеганография как теория скрытия информации получила новый импульс к развитию. В настоящее время методы стеганографии условно делят на:

- классическую стеганографию — включает в себя «некомпьютерные методы»;
- компьютерная стеганографию — направ-

ление классической стеганографии, основанное на реализации методов стеганографии на основе вычислительных и телекоммуникационных платформ и использования специальных свойств обрабатываемых и передаваемых форматов данных;

– цифровую стеганографию — направление компьютерной стеганографии, основанное на сокрытии информации в цифровых объектах, изначально имеющих аналоговую природу (изображения, видео, звуки).

В работах [1-3] показано, что к основным направлениям приложения современной теории

компьютерной стеганографии относятся следующие:

- организация стеганографических (скрытых) систем связи на основе современных телекоммуникационных систем и противодействие им;
- обеспечение целостности и подлинности информационных ресурсов за счет встраивания цифровых водяных знаков;
- обеспечение целостности и идентификации информационных ресурсов за счет встраивания идентификационных номеров;
- дополнение информационных ресурсов за счет встраивания в них заголовков.

Однако анализ основных монографий [1-3], некоторых публикаций [4-6], а также диссертационных исследований [7-17] в предметной области компьютерной стеганографии показал, что ее современная теория обладает рядом недостатков, позволяющих обосновать новые направления ее дальнейшего развития:

- не устоявшийся и неоднозначный терминологический базис;
- глубокая проработанность теоретических основ создания стегосистем и недостаточное исследование аспектов проведения атак на стеганографические системы;
- широкое освещение теоретических вопросов, посвященных цифровым водяным знакам, при недостаточной проработанности теории построения стеганографических систем связи с использованием имеющегося задела в теории передачи информации, теории систем связи, теории информационной безопасности.

В данной статье предлагается эталонная модель, направленная на устранение последнего из вышеуказанных недостатков, которая может быть использована как для формализованного описания уже известных стеганографических систем, так и для создания принципиально новых решений в данной области, часть которых представлена ниже.

В теории систем связи основой формализованного описания взаимодействия абонентов составляет эталонная модель взаимодействия открытых систем (OSI – open systems interconnection) [18]. Декомпозиция информационного обмена абонентов посредством систем связи на уровни позволило формализовать различные аспекты взаимодействия абонентов, разделяя их в соответствии с функционалом решаемых задач. Предлагается перенести подход к декомпозиции взаимодействия абонентов на различные уровни, используемый в модели OSI, на взаимодействие абонентов стеганографической системы связи, с учетом особенностей последней.

Для описания взаимодействия абонентов стеганографической системы связи в рамках предлагаемой эталонной модели предлагается определиться с терминологическим базисом в рамках которого будет вестись описание модели.

На основе известного понятийного аппарата теории передачи информации, теории систем связи, теории информационной безопасности предлагается уточнить семантическую область ряда применяемых в теории стеганографии терминов (выделены курсивом), а также ввести новые понятия, ранее в этой области не используемые.

**Сообщение** – скрытно передаваемая информация.

**Контейнер (стегоконтейнер)** – информация, в которую встраивается тайное сообщение. Пустой контейнер – контейнер, не содержащий скрытого сообщения. Заполненный контейнер (стегоконтейнер) – контейнер, содержащий скрытое сообщение.

**Стегоключ** – секретный ключ, используемый для сокрытия сообщения в стегоконтейнере.

**Стеганографическая связь (стегосвязь)** – скрытый обмен сообщениями за счет их встраивания в другую информацию, передаваемую по системе связи.

**Вид стегосвязи** – классификационная группа стегосвязи, выделяемая по виду передаваемого сообщения (данные, текст, голос, видео, изображение и др.).

**Род стегосвязи** – классификационная группа стегосвязи, выделяемая по виду контейнера в который встраивается сообщения (данные, текст, голос, видео, изображение и др.).

**Абонент системы стеганографической связи** – отправитель или получатель скрытых сообщений.

**Стеганографическая система связи (стегосистема)** – совокупность взаимоувязанных и согласованных по задачам, месту и времени методов и средств, стегоузлов и стегоканалов функционирующих в интересах обслуживания абонентов, ведущих скрытый обмен сообщениями.

**Узел стеганографической связи (стегоузел)** – элемент стегосистемы, представляющий собой объединение методов и средств для образования стегоканалов, их распределении и коммутации, извлечения и встраивания сообщений, передаваемых по стегоканалам различного рода, а также предоставление абонентам стегосистемы услуг по скрытому обмену сообщениями.

**Канал стеганографической связи (стегоканал)** – объединение методов и средств (стегокодер, стегодетектор, стегодекодер), используемых для создания определенного рода стегосвязи

между стегоузлами. В традиционных работах по стеганографии ранее данному определению соответствовало понятие стегосистемы.

**Стегокодер** – устройство, предназначенное для осуществления вложения скрытого сообщения в контейнер.

**Стегодетектор** – устройство, предназначенное для определения наличия сообщения в контейнере.

**Стегодекодер** – устройство, восстанавливающее скрытое сообщение из контейнера.

**Сеть стеганографической связи (стегосеть)** – совокупность узлов стегосистемы и соединяющих их стегоканалов.

**Направление стеганографической связи (стегонаправление)** – совокупность стегоканалов и стегоузлов, обеспечивающих стегосвязь между двумя абонентами.

**Система управления стеганографической связью** – часть стегосистемы, обеспечивающая функционирование ее с заданным качеством.

**Качество стеганографической связи** – свойство стегосвязи, по обеспечению своевременной и достоверной передаче сообщений.

**Своевременность стеганографической связи** – способность стегосвязи обеспечивать передачу сообщений по стегосистеме в заданное время.

**Достоверность стеганографической связи** – способность стегосвязи обеспечивать воспроизведение передаваемых сообщений в пунктах приема с заданной точностью.

**Готовность элемента стегосистемы** – состояние элемента стегосистемы, характеризующее степень его готовности к выполнению своих функций по обеспечению стегосвязи.

**Пропускная способность стегосистемы** – максимальное количество сообщений (информации), которое с заданным качеством может передать стегосистема за единицу времени.

**Стегоанализ** – процесс определения факта наличия стегосвязи и параметров стегосистемы.

**Атака на стегосистему** – активные или пассивные действия противника/нарушителя по стегоанализу, нарушению корректного функционирования стегосистемы, уничтожению, искажению либо подмене передаваемых по ней сообщений.

**Стеганографическая стойкость (стегостойкость)** – свойство, определяющее способность стегоконтейнера и скрытого в нем сообщения противостоять возможным атакам на них. Стеганографическую стойкость традиционно рассматривают в трех аспектах, соответствующих передаче сообщений в контейнере:

- невозможность определения факта нахождения скрытого сообщения в стегоконтейнере (скрытность сообщения);

- невозможность извлечения данных из стегоконтейнера, при определении факта наличия стегоконтейнера;

- невозможность прочтения сообщения после извлечения данных из стегоконтейнера.

**Стеганографическая скрытность (стегоскрытность)** – свойство стегосистемы и ее отдельных элементов, по способности обеспечивать невозможность определения факта ведения стегосвязи. Предлагается отличать стегоскрытность от стегостойкости, так как понятие стегоскрытности характеризует свойство скрытности применительно не к стегоконтейнеру, а к таким объектам как стегоканал, стегосеть, стегосистема.

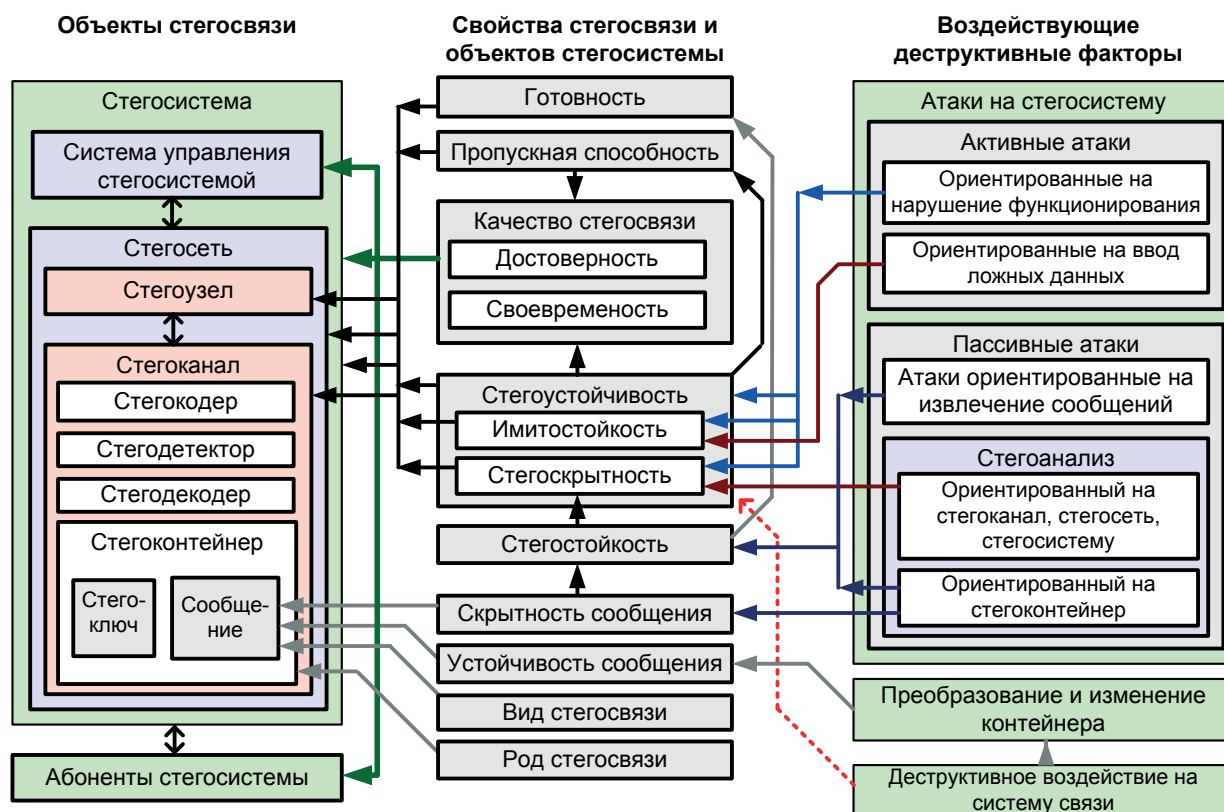
**Устойчивость стегосистемы (стегоустойчивость)** – свойство, определяющее способность стегосистемы и ее отдельных элементов обеспечить заданное качество стегосвязи в условиях воздействия различных деструктивных факторов и атак на нее. Предлагается различать свойство устойчивости (отличительным признаком которой является наличие условий воздействия различных деструктивных факторов и атак, направленных на нарушение функционирования стегосистемы), от свойства скрытности (отличительным признаком которой является условия проведения атак направленных на выявление факта стегосвязи).

**Устойчивость сообщения** – свойство сообщения, определяющее возможность его воспроизведения в пунктах приема с заданным уровнем достоверности, в условиях преобразования и изменения параметров контейнера.

**Имитостойкость стегосистемы** – способность стегосистемы противостоять вводу в нее ложных, в том числе и ранее переданных, сообщений, а также навязыванию ей ложных режимов работы.

Взаимосвязь представленных понятий для объектов стегосистемы, свойств стегосистемы и стегосвязи, а также для характерных в данной предметной области деструктивных воздействий представлено на рис. 1.

На основе этих понятий предлагается formalизовать взаимодействие абонентов стеганографической системы связи в виде многоуровневой эталонной модели взаимодействия стеганографических систем - **ЭМБСС (Steganographically Systems Interconnection basic reference model – SSI model)**. Данная эталонная модель позволяет обобщить имеющиеся работы в области стеганографического сокрытия сообщений в контейнерах [1-15, 19] и органично развить направления работ [8, 16, 17, 20-22] в направлении создания единой формализованной модели стегосистемы, как одного из вариантов реализации системы



**Рис. 1.** Взаимосвязь представленных определений объектов стегосистемы, свойств стегосистемы и стегосвязи, а также характерных для данной предметной области деструктивных воздействий

скрытой передачи сообщений, наложенной на телекоммуникационную систему связи.

На первом уровне ЭМВСС (уровень системы связи) рассматривается система связи, реализующая информационный обмен контейнерами. Этот уровень описывается в соответствии с семиуровневой моделью OSI [18]. Также на данном уровне предлагается формализовать модели доступа к системе связи и воздействия на нее нарушителя/противника в соответствии со стандартными моделями информационной безопасности [23].

На втором уровне ЭМВСС (уровень стегоконтейнера) предлагается формализовать процессы, связанные с встраиванием и извлечением сообщения в контейнер, процессы формирования и управления ключевой информацией на уровне отдельных контейнеров. Здесь же предлагается формализовать вопросы устойчивости сообщений к преобразованию контейнера, а также учитывать различные рода стегосвязи. На данном уровне предлагается описать методы стегоанализа, направленные на вскрытие факта нахождения сообщения в контейнере, а также атаки (как активные, так и пассивные) направленные на контейнер и передаваемое в нем сообщение. Отдельные показатели и критерии, описывающие свойства и эффективность формализуемых на данном

уровне процессов, в частности понятие стеганографической стойкости, тоже соответствует данному уровню модели ЭМВСС.

Проведенный анализ работ по теории стеганографии показал, что подавляющее их количество соответствует формализации процессов на уровне стегоконтейнера и рассматривает различные аспекты встраивания сообщений в видео- [1, 19], аудио- [1-3, 7, 9], графические данные [1-3, 9-12, 14, 15], текст [3], а так же в различные служебные поля и заголовки пакетов систем связи [1-3, 8, 13]. Работы по стегоанализу и атакам, направленным на контейнеры различного рода [1-3, 4-6], также могут быть отнесены к данному уровню.

На третьем уровне ЭМВСС (уровень стегоканала) предлагается формализовать процессы, связанные с образованием стегоканалов различных родов; процессы стегокодирования, стегодетектирования, стегодекодирования в стегоканале; управления в стегоканалах ключевой информацией для отдельных контейнеров (соответственно - объемом и стеганографической стойкостью сообщений); разделения стегоканала и множественного доступа абонентов к нему, а также параметры отдельного стегоканала: скрытность, пропускная способность, своевременность, устойчивость. На этом уровне предлагается описать задачи стегоа-



нализа по выявлению факта наличия стегоканала, а также атаки направленные на стегоканал.

Анализ опубликованных работ показал, что в большинстве исследований рассматривается моно-стегоканал, без учета возможности его разделения между абонентами, или предоставления к нему множественного доступа. В частности, среди открытых работ только в работах [19, 22] рассматривается вариант кодового множественного доступа к стегоканалу [19] и пространственно-временное разделение стегоканала [22]. При этом основной характеристикой стегоканала считают пропускную способность [1, 3], без учета характеристик его своевременности и устойчивости. Также в имеющихся работах присутствует путани-

ца с применением понятия «стеганографической стойкости». В связи с этим понятие «стеганографическая стойкость» в том контексте в котором она рассматривается в работах [1-5] предлагается целиком отнести к уровню стегоконтейнера, а на уровне стегоканала оперировать понятиями устойчивости и скрытности стегоканала, определение которых предложено в данной работе.

На четвертом уровне ЭМВСС (уровень стегосети) предлагается ввести новые понятия стегосети и стегоузла и формализовать процессы, соответствующие скрытому обмену сообщениями по множеству стегоканалов, входящих в стегосеть, а также процессы преобразования сообщений в стегоузлах. К процессам, формализуемым на

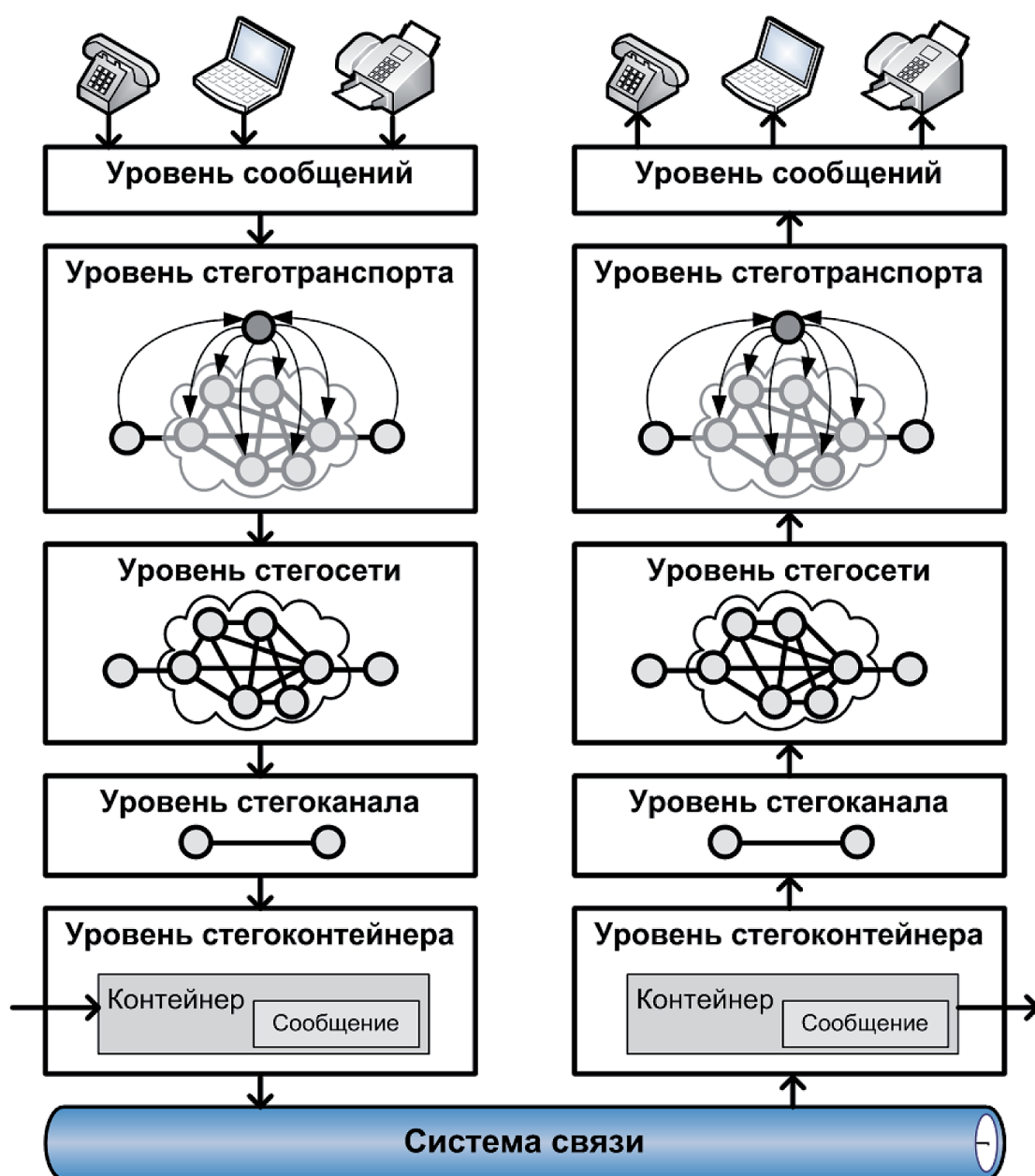


Рис. 2. Структура взаимодействия уровней ЭМВСС

## Эталонная модель взаимодействия стеганографических систем

*Таблица. Предложения по формализации объектов, предметов и различных аспектов взаимодействия абонентов стеганографической системы на уровнях ЭМВСС*

№	Уровни модели	Объекты и предметы стеганографической системы
1	Уровень системы связи	<b>Объекты уровня</b> Система связи, реализующая передачу стегоконтейнера. Противник/нарушитель. <b>Предметы уровня</b> Методы обеспечения заданного качества функционирования системы связи в соответствии с моделью OSI.
2	Уровень стегоконтейнера	<b>Объекты уровня стегоконтейнера</b> Стегоконтейнер. Сообщение. <b>Предметы уровня стегоконтейнера</b> Метод встраивания сообщений в стегоконтейнер. Методы формирования ключевой информации. Методы обеспечения заданного уровня устойчивости сообщений в условиях преобразования и изменения параметров контейнера. Методы обеспечения стеганографической стойкости и ее аспекты на уровне стегоконтейнера. Методы стегоанализа контейнера. Методы проведения атак на стегоконтейнер.
3	Уровень стегоканала	<b>Объекты уровня</b> Стегоканал. Параметры стегоканала: скрытность, пропускная способность, своевременность, устойчивость. Абоненты стегоканала. <b>Предметы уровня</b> Методы множественного доступа абонентов к стегоканалу. Методы управления ключевой информацией контейнеров. Методы стегоанализа стегоканала. Методы проведения атак на стегоканал.
4	Уровень стегосети	<b>Объекты уровня</b> Стегосеть. Абоненты, узлы и стегоканалы стегосети. <b>Предметы уровня</b> Методы объединения стегоканалов в стегосеть. Методы управления параметрами и ключевой информацией стегоканалов. Методы маршрутизации сообщений в стегоузлах по стегоканалам. Методы преобразования сообщений в узлах сетгосети. Методы оценки, измерения и контроля параметров стегоканалов в стегосети. Методы обеспечения устойчивости и скрытности потоков сообщений в стегосетях. Методы стегоанализа стегосетей. Методы проведения атак на стегосети.
5	Уровень стеготранспорта	<b>Объекты уровня</b> Абоненты стеганографической системы связи. Информационные направления стегосвязи. <b>Предметы уровня</b> Методы обеспечения заданной своевременности, пропускной способности, устойчивости, скрытности при передаче сообщений по стегонаправлениям связи. Методы управления ресурсами и параметрами стегосети для обеспечения заданного качества обслуживания при передаче сообщений.
6	Уровень сообщений	<b>Объекты уровня</b> Виды информации представляемые к передаче в виде сообщений. <b>Предметы уровня</b> Требования по качеству обслуживания информации передаваемой в виде сообщений. Методы разборки/сборки сообщений конечными абонентами. Методы борьбы с ошибками потери или дублирования сообщений с учетом вида передаваемой информации.

данном уровне, целесообразно отнести: объединение отдельных стегоканалов в стегосеть, маршрутизацию сообщений по стегоканалам, преобразование сообщений в стегоузлах. На данном уровне предлагается формализовать: методы оценки, измерения и контроля параметров отдельных стегоканалов в стегосети; методы управления параметрами и ключевой информацией отдельных стегоканалов; методы обеспечения устойчивости и скрытности потоков сообщений в стегосетях. Модели противника/нарушителя, методы стегоанализа и проведения атак, ориентированных на стегосети в целом, также стоит отнести к данному уровню.

На пятом уровне ЭМБСС (уровень стеготранспорта) предлагается ввести новое понятие «направление стегосвязи» как совокупности стегоканалов и стегоузлов обеспечивающих стегосвязь между двумя абонентами и отнести к данному уровню: вопросы управления ресурсами и параметрами стегосети и отдельных стегоканалов для обеспечения заданного качества обслуживания сообщений; методы и средства обеспечения заданной своевременности, пропускной способности, устойчивости и скрытности при передаче сообщений по направлениям стегосвязи, в том числе в условиях стегоанализа и атак нарушителя. При формализации и классификации решаемых задач управления ресурсами стегосети предлагается взять за основу концепцию управления TMN (Telecommunication Management Network), в дальнейшем модифицировав ее с учетом особенностей стегосвязи.

На шестом уровне ЭМБСС (уровень сообщений) предлагается рассмотреть: требования конечных абонентов сети к качеству обслуживания передаваемых ими сообщений; виды информации (данные, голос, видео, изображения) представляемые к встраиванию в виде сообщений; требования к параметрам и качеству обслуживания сообщений, содержащих соответствующий вид информации, в том числе и особенности разборки/сборки сообщений передаваемой информации абонентами стегосистемы. Предполагается, что требования к качеству обслуживания сообщений являются входными ограничениями для методов управления рассматриваемых на уровне стеготранспорта.

В настоящее время работы, соответствующие процессам, формализованным в рамках предлагаемой модели ЭМБСС на уровнях стегосети, стеготранспорта и стегосообщений, автору неизвестны.

Предложения по уровням модели ЭМБСС и формализации объектов, предметов и различных

аспектов взаимодействия абонентов стеганографической системы связи на данных уровнях представлены на рис. 2. и в таблице.

В таблице, ранее отсутствующие элементы научно-методического аппарата описания взаимодействия стеганографических систем выделены курсивом.

Перенос в модель ЭМБСС части функциональных особенностей из модели OSI позволил:

- обобщить в формализованном виде существующие теоретические основы построения, функционирования и анализа стеганографических систем;

- предложить новые направления развития стеганографических систем, на основе которых могут быть обоснованы принципиально новые прикладные решения.

В частности, к новым направлениям прикладного развития стеганографических систем связи, которые могут быть основаны на вышеприведенной модели, можно отнести:

- существенное увеличение пропускной способности направлений стегосвязи за счет использования многоканальной передачи сообщений, с одновременным повышением скрытности отдельных стегоканалов, за счет уменьшения объема сообщений, передаваемых по каждому конкретному стегоканалу;

- передача голосовой, видео и графической информации при разборке их на сообщения с учетом вида информации, и последующей их передачей с обеспечением качества обслуживания сообщений в направлениях стегосвязи с заданной пропускной способностью;

- построение распределенных в информационном пространстве стеганографических систем связи в которых обеспечение заданного уровня устойчивости и скрытности обеспечивается значительным наращиванием связности топологии стегосетей и направлений стегосвязи, с одновременным снижением пропускной способности отдельных стегоканалов, и объема встраиваемых сообщений;

- построение адаптивных к действиям нарушителя/противника стегосистем за счет реализации новых методов и способов управления ресурсами стегосистем и ключевой информацией в них;

- разработка новых способов стегоанализа, направленных на вскрытие факта существования, а также противодействие стегосетям и направлениям стегосвязи.

Таким образом, предложенная модель ЭМБСС может быть использована не только для обобщения и развития теории стеганографических систем, но может быть положена в основу принципиаль-

но новых алгоритмических, программных и технических решений по созданию стегосистем.

Предложенная в работе терминология и обобщенная модель ЭМВСС не являются окончатель-

ными, носят дискуссионный характер и автор надеется, что они найдут свое дальнейшее развитие и будут востребованы специалистами в области стеганографии.

### Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.
2. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стегоанализ. Монография. М.: Вузовская книга, 2009. 220 с.
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
4. Разинков Е.В., Латыпов Р.Х. Стойкость стеганографических систем // Ученые записки Казанского гос. ун.-та. Физ.-мат. науки. 2009. Т. 151. Кн. 2. С. 126-132.
5. Ремизов А.В., Филиппов М.В. Оценка необнаружимости стеганографических алгоритмов // Наука и образование. 2012. № 3. URL: <http://technomag.edu.ru/doc/359383.html> (дата доступа 17.04.2014)
6. Сизов А.С., Никутин Е.И., Котенко С.В. Обзор и тенденции развития методов анализа стеганографических систем // Известия Юго-Западного государственного университета. Серия Управление, вычислительная техника, информатика. Медицинское приборостроение. 2013. № 4. С. 43-48.
7. Аленин А.А. Разработка и исследование методов скрытой передачи информации в аудиофайлах. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.15. Самара: ПГУТИ, 2011. 174 с.
8. Алиев А.Т. Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Ростов-на-Дону: ЮФУ, 2008. 216 с.
9. Дрюченко М.А. Статистические и нейросетевые алгоритмы синтеза и анализа стеганографически скрытой информации в аудио- и графических данных. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.17. Воронеж: ВГУ, 2010. 192 с.
10. Жилкин М.Ю. Теоретико-информационные методы стегоанализа графических данных. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Новосибирск: СибГУТИ, 2009. 153 с.
11. Кувшинов С.С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. СПб.: НИУ ИТМО, 2010. 116 с.
12. Мерзлякова Е.Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Новосибирск: СибГУТИ, 2011. 161 с.
13. Пономарев К.И. Некоторые математические модели стеганографии и их статистический анализ. Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 01.01.05. М.: МИЭМ, 2010. 81 с.
14. Разинков Е.В. Математическое моделирование стеганографических объектов и методы вычисления оптимальных параметров стегосистем. Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 05.13.18. Казань: КГУ, 2012. 109 с.
15. Рублев Д.П. Разработка и исследование высокочувствительных методов стегоанализа. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.19. Таганрог: ТТИ ЮФУ, 2007. 139 с.
16. Жгун А.В. Модель скрытой передачи информации в каналах связи. Дисс. на соиск. уч. ст. канд. ф.-мат. наук по спец. 05.13.18. В. Новгород: НовГУ, 2003. 187 с.
17. Жгун А.А. Модель скрытой передачи информации для дискретных каналов с повышенным уровнем помех. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.13.18. В. Новгород: НовГУ, 2010. – 216 с.
18. Макаренко С.И. Вычислительные системы, сети и телекоммуникации: учебное пособие. Ставрополь: СФ МГТУ им. М. А. Шолохова, 2008. 352 с.
19. Абазина Е.С. Формирование стеганографического канала с кодовым уплотнением на основе двумерных нелинейных сигналов // Вопросы радиоэлектроники в сфере техники телевидения. 2014. № 1. С. 73-81.
20. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Самара: ПГУТИ, 2012. 166 с.
21. Макаров М.И. Разработка и исследование методов скрытой распределенной передачи сеансовых данных в телекоммуникационных сетях. Дисс. на соиск. уч. ст. канд. техн. наук по спец. 05.12.13. Самара: ПГУТИ, 2013. 144 с.
22. Алексеев А.П., Макаров М.И. Принципы многоуровневой защиты информации // Инфокоммуникационные технологии. 2012. Т. 10. № 2. С. 88-93.
23. Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГТУ им. М.А. Шолохова, 2009. 372 с.

### Reference

1. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaja steganografija. M.: Solon-Press, 2009. 272 s. [Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography. Moscow: Solon-Press, 2009. 272 p. (In Russia)]
2. Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganografija, cifrovye vodjanye znaki i stegoanaliz. Monografija. M.: Vuzovskaja kniga, 2009. 220 s. [Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganography, digital water marks and stegoanalysis. Treatise. Moscow: Vuzovskaja kniga, 2009. 220 p. (In Russia)]
3. Konahovich G.F., Puzyrenko A.Ju. Komp'juternaja steganografija. Teorija i praktika. K.: MK-Press, 2006. 288 s. [Konahovich G.F., Puzyrenko A.Ju. Computer-held steganography. Theory and practice. Kiev: MK-Press, 2006. 288 p. (In Russia)]
4. Razinkov E.V., Latypov R.H. Stojkost' stegonograficheskikh system // Uchenye zapiski Kazanskogo Universiteta. Seria Fiziko-Matematicheskie Nauki. 2009. T. 151. Kn. 2. S. 126-132. [Razinkov E.V., Latypov R.H. The constancy of steganographic systems // Uchenye zapiski Kazanskogo Universiteta. Seria Fiziko-Matematicheskie Nauki. 2009. Vol. 151/2. pp. 126-132. (In Russia)]
5. Remizov A.V., Filippov M.V. Ocenka neobnaruzhimosti steganograficheskikh algoritmov // Nauka i obrazovanie. 2012. № 3. URL: <http://technomag.edu.ru/doc/359383.html> (data dostupa 17.04.2014) [Remizov A.V., Filippov M.V. The rating of nondetectable



- steganographic algorithms // Nauka i obrazovanie. 2012. № 3. URL: <http://technomag.edu.ru/doc/359383.html>]
6. Sizov A.S., Nikutin E.I., Kotenko S.V. Obzor i tendencii razvitiya metodov analiza steganograficheskikh sistem // Izvestiya Jugo-Zapadnogo gosudarstvennogo universiteta. Seriya Upravlenie, vychislitel'naya tekhnika, informatika. Medicinskoe priborostroenie. 2013. № 4. S. 43-48. [Sizov A.S., Nikutin E.I., Kotenko S.V. Overview and trends of the analysis methods of steganographic messages development // Proceedings of the southwest state university. 2013. № 4. pp. 43-48. (In Russia)]
  7. Alenin A.A. Razrabotka i issledovanie metodov skrytoy peredachi informacii v audiofajlah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.15. Samara: PGUTI, 2011. 174 s. [Alenin A.A. The development and analysis of nondetectable data communication in audio files` methods. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2011. 174 p. (In Russia)]
  8. Aliev A.T. Razrabotka modelej, metodov i algoritmov perspektivnykh sredstv zashhity informacii v sistemah jelektronnoho dokumentooborota na baze sovremennykh tekhnologij skrytoj svyazi. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19 Rostov-na-Donu: JuFU, 2008. 216 s. [Aliev A.T. The development of models, methods and algorithms of perspective data protection means in electronic document management systems, based on present-day technologies of nondetectable data communication. Diss. Ph.D. Rostov-na-Donu: South Federal University, 2008. 216 p. (In Russia)]
  9. Drjuchenko M.A. Statisticheskie i nejrosetevye algoritmy sinteza i analiza steganograficheskij skrytoj informacii v audio- i graficheskikh dannykh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.17. Voronezh: VGU, 2010. 192 s. [Drjuchenko M.A. Statistical and neuronet algorithms of synthesis and analysis of steganographically nondetectable data in audio and graphic files. Diss. Ph.D. Voronezh: Voronezh State University, 2010. 192 p. (In Russia)]
  10. Zhilkin M.Ju. Teoretiko-informacionnye metody stegoanaliza graficheskikh dannykh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Novosibirsk: SibGUTI, 2009. 153 s. [Zhilkin M.Ju. Information-theoretical methods of stegananalysis of graphic data. Diss. Ph.D. Novosibirsk: Siberian State University of Telecommunications and Information Sciences, 2009. 153 p. (In Russia)]
  11. Kuvshinov S.S. Metody i algoritmy sokrytija bol'shih ob'emov dannykh na osnove steganografii. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. SPb.: NIU ITMO, 2010. 116 s. [Kuvshinov S.S. Methods and algorithms of big data` hiding based on steganography. Diss. Ph.D. St. Petersburg: Saint-Petersburg National Research University of Information technologies, mechanics and Optics, 2010. 116 p. (In Russia)]
  12. Merzljakova E.Ju. Postroenie steganograficheskikh sistem dlja rastrovnykh izobrazhenij, bazirujushhijhsja na teoretiko-informacionnykh principah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. Novosibirsk: SibGUTI, 2011. 161 s. [Merzljakova E.Ju. Steganographic systems` development for bit-map images, based on –theoretic-informational concepts. Diss. Ph.D. Novosibirsk: Siberian State University of Telecommunications and Information Sciences, 2011. 161 p. (In Russia)]
  13. Ponomarev K.I. Nekotorye matematicheskie modeli steganografii i ih statisticheskij analiz. Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 01.01.05. M.: MIJeM, 2010. 81 s. [Ponomarev K.I. Some mathematical.../user/AppData/Local/Temp/1406428456 models of steganography and statistical analysis of them. Diss. Ph.D. Moscow: Moscow Institute of Economics and Mathematics. 2010. 81 p. (In Russia)]
  14. Razinkov E.V. Matematicheskoe modelirovanie steganograficheskikh ob'ektov i metody vychislenija optimal'nykh parametrov stegosistem. Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 05.13.18. Kazan': KGU, 2012. 109 s. [Razinkov E.V. The mathematical modeling of steganographic objects and methods of optimal parameters of steganographic systems` calculation. Diss. Ph.D. Kazan: Kazan State University, 2012. 109 p. (In Russia)]
  15. Rublev D.P. Razrabotka i issledovanie vysokochuvstvitel'nykh metodov stegoanaliza. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.19. Taganrog: TTI JuFU, 2007. 139 s. [Rublev D.P. The development and analysis of highly sensitive methods of stegananalysis. Diss. Ph.D. Taganrog: Taganrog Institute of Radio Engineering, 2007. 139 p. (In Russia)]
  16. Zhgun A.V. Model' skrytoj peredachi informacii v kanalah svyazi. Diss. na soisk. uch. st. kand. f.-mat. nauk po spec. 05.13.18. V. Novgorod: NovGU, 2003. 187 s. [Zhgun A.V. The model of nondetectable data communication. Diss. Ph.D. Gteat Novgorod: Novgorod State University, 2003. 187 p. (In Russia)]
  17. Zhgun A.A. Model' skrytoj peredachi informacii dlja diskretnykh kanalov s povyshennym urovnem pomeh. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.13.18. V. Novgorod: NovGU, 2010. 216 s. [Zhgun A.V. The model of nondetectable data communication for the channels with raised level of noise. Diss. Ph.D. Gteat Novgorod: Novgorod State University, 2010. 216 p. (In Russia)]
  18. Makarenko S.I. Vychislitel'nye sistemy, seti i telekommunikacii: uchebnoe posobie. Stavropol': SF MGGU im. M. A. Sholohova, 2008. 352 s. [Makarenko S.I. Computer systems, networks and telecommunication: Tutorial. Stavropol: Sholokhov Moscow State University for the Humanities (Stavropol branch), 2008. 352 p. (In Russia)]
  19. Abazina E.S. Formirovanie steganograficheskogo kanala s kodovym uplotneniem na osnove dvumernykh nelinejnykh signalov // Voprosy radioelektroniki. Seria: tekhnika televidenija. 2014. № 1. S. 73-81. [Abazina E.S. Forming of stenography data link with code consolidation based on two-dimensional nonlinear signals // Voprosy radioelektroniki. Seria: tekhnika televidenija. 2014. № 1. pp. 73-81.]
  20. Orlov V.V. Metody skrytoj peredachi informacii v telekommunikacionnykh setjah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Samara: PGUTI, 2012. 166 s. [Orlov V.V. Methods of nondetectable data communication in telecommunication networks. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2012. 166 p. (In Russia)]
  21. Makarov M.I. Razrabotka i issledovanie metodov skrytoj raspredelennoj peredachi seansovykh dannykh v telekommunikacionnykh setjah. Diss. na soisk. uch. st. kand. tehn. nauk po spec. 05.12.13. Samara: PGUTI, 2013. 144 s. [The development and analysis of methods of nondetectable allocated session data in telecommunication networks. Diss. Ph.D. Samara: Povolzhskiy State University of Telecommunications and Informatics, 2013. 144 p. (In Russia)]
  22. Alekseev A.P., Makarov M.I. Principy mnogourovnevoj zashhity informacii // Infokommunikacionnye tekhnologii. 2012. T. 10. № 2. S. 88-93. [Alekseev A.P., Makarov M.I. Principles of multilevel protection of the information // Infokommunikacionnye tekhnologii. 2012. Vol. 10. № 2. pp. 88-93. (In Russia)]
  23. Makarenko S.I. Informacionnaja bezopasnost': uchebnoe posobie dlja studentov vuzov. Stavropol': SF MGGU im. M.A. Sholohova, 2009. 372 s. [Makarenko S.I. Information security: Tutorial. Stavropol: Sholokhov Moscow State University for the Humanities (Stavropol Branch), 2009. 372 p. (In Russia)]



# АНАЛИЗ ЗАВИСИМОСТИ УРОВНЯ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ СВЯЗИ ОТ ЭКСПЕРТНЫХ ДАННЫХ ПРИ РАСЧЕТАХ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ НЕЧЕТКИХ МНОЖЕСТВ

*Бельфер Рувим Абрамович, кандидат технических наук, доцент  
Калюжный Денис Александрович  
Тарасова Дарья Владимировна*

*В работе анализируется влияние экспертных данных на оценку уровня риска угроз информационной безопасности (ИБ) в сетях связи при расчете значений риска этих угроз с помощью модели нечетких множеств. В качестве таких данных рассматривались функции принадлежности, терм-множество, продукционные правила. Расчет производился на примерах нескольких угроз фрода в сети VoIP стандарта сигнализации SIP.*

**Ключевые слова:** информационная безопасность, фрод, угроза, нечеткое множество, оценка риска, уровень риска угрозы, протокол установления сеанса связи (сигнализации), вероятность реализации угрозы, ущерб, функция принадлежности, терм-множество, экспертная оценка; лингвистическая переменная

## ANALYSIS OF DEPENDENCE OF RISK LEVEL OF SAFETY OF COMMUNICATION NETWORKS ON EXPERT DATA DURING CALCULATIONS WITH THE USE OF A MODEL OF THE ILLEGIBLE SETS

*Ruvim Belfer, Ph.D, Associate Professor  
Denis Kalyuzhnyy  
Daria Tarasova*

*This paper analyzes the impact of expert data on the risk assessment of information security (IS) threats in communication networks when calculating the risk of information security threats with a model of fuzzy sets. As these data were considered membership function, term set, production rules. The calculation is made on the examples of several threats of fraud in the VoIP network signaling standard SIP.*

**Keywords:** information security; fraud; threat; fuzzy set; risk; risk level of threat; protocol SIP (Session Initialization Protocol likelihood of occurrence; impact; membership function; term set; linguistic variable.

### Введение

Согласно стандарту международного союза электросвязи (ITU-T) E.408 [ITU-T. Recommendation E.408. Telecommunication Network Security Requirement, 2004] количественная оценка риска угрозы ИБ в сети связи, определяется двумя характеристиками – вероятностью угрозы и последствием при реализации этой угрозы (т.е. ущербом). На основании значений риска угроз ИБ производится их ранжирование по уровню риска угрозы ИБ. Это позволяет при проектировании, испытаниях и эксплуатации сети наибольшее вни-

мание уделять обеспечению защиты от угроз ИБ с наиболее высокими уровнями риска.

В основу некоторых работ по вычислению риска угрозы ИБ в сети связи положена модель с использованием теории нечетких множеств и нечеткой логики [1]. К ним относится работа [2] безотносительно конкретной сети связи, а также работы относительно следующих сетей связи:

- беспроводной сети стандарта IEEE 802.11 [3];
- транспортная сеть VANET [4].

Для этой модели расчета характерно использование многих данных нечетких множеств, по-

лученных с помощью субъективных оценок экспертным методом.

В настоящей работе на основе модели с использованием теории нечетких множеств и нечеткой логики приводится определение количественной характеристики риска угрозы ИБ в сети связи. Практическим результатом использования полученных значений риска угроз ИБ является их ранжирование [3,5]. Это дает возможность принять первоочередные меры по усилению защиты от угроз ИБ с наиболее высокими уровнями риска.

*Задача настоящей работы показать возможную погрешность определения риска нескольких угроз ИБ и соответственно результатов ранжирования уровней риска этих угроз, вызванную субъективностью некоторых экспертных данных в модели с использованием теории нечетких множеств и нечеткой логики. Анализ подлежат влияние только тех экспертных данных, которые используются этим математическим аппаратом при определении риска угрозы ИБ. Этому посвящен раздел 2 статьи.*

В разделе 1 настоящей статьи приводится пример расчета риска одной из угроз ИБ, в основу которого положена методика в работе [3], используемая для беспроводных сетей стандарта IEEE 802.11.

### 1. Расчет риска угрозы ИБ сети связи

Определение риска угрозы ИБ на основе теории нечетких множеств состоит из следующих последовательных этапов: описание угроз ИБ сети, формализация лингвистической переменной вероятности реализации угрозы, формализация лингвистической переменной ущерба реализации угрозы ИБ, фазификация, дефазификация, оценка риска угрозы ИБ.

На первом этапе необходимо определить угрозы ИБ сети, для которых производится оценка риска. В настоящей работе примем угрозы фрода в сигнализации по протоколу SIP сети передачи речи и данных поверх IP (Voice over IP, VoIP) [6]. Примером могут быть некоторые угрозы фрода, приведенные в работах [7,8]: мошенничество с подпиской, перехват и кража подписки, мошеннический обход, манипуляция сигнальными сообщениями, использование уязвимостей в учрежденческих станциях и в системе голосовой почты, распределение дохода между операторами и др.

На основе модели с использованием теории нечетких множеств и нечеткой логики для примера определим значение риска одной из угроз фрода в сети сигнализации SIP.

### 1.1. Формализация лингвистических переменных вероятности реализации угрозы ИБ и ущерба угрозы ИБ

Как было отмечено выше, в настоящей работе при определении риска угрозы ИБ и соответствующего уровня риска угрозы ИБ анализу подлежат влияние на возможную погрешность только тех экспертных данных, которые используются аппаратом теории нечетких множеств и нечеткой логики. По этой причине влияние экспертных данных при определении вероятностей при реализации угроз и ущерба при реализации угроз не рассматривается. Для приведенного ниже примера расчета риска рассмотрим угрозу фрода с соответствующими параметрами: вероятность реализации  $P=0.83$  и ущерб при реализации  $U=0.4$ .

Для анализа риска угрозы фрода на основе модели с использованием теории нечетких множеств и нечеткой логики необходимо формализовать лингвистические переменные вероятности реализации угрозы или ущерба. Нечетким множеством (fuzzy set)  $\tilde{A}$  на универсальном множестве  $U$  называется совокупность пар  $(\mu_A(u), u)$ , где  $\mu_A(u)$  - степень принадлежности элемента  $u \in U$  к нечеткому множеству. Степень принадлежности - это число из диапазона  $[0, 1]$ . Чем выше степень принадлежности, тем в большей мере элемент универсального множества соответствует свойствам нечеткого множества. Лингвистической переменной (linguistic variable) называется переменная, значениями которой могут быть слова или словосочетания некоторого естественного или искусственного языка. Терм-множеством (term set) называется множество всех возможных значений лингвистической переменной. Для лингвистической переменной вероятности реализации угрозы фрода для настоящего примера определим следующие терм-множества: низкая, средняя и высокая. Для лингвистической переменной ущерба при реализации угрозы фрода для настоящего примера определим следующее терм-множество: незначительный, малый, средний, существенный, недопустимый.

Термом (term) называется любой элемент терм-множества. В теории нечетких множеств терм формализуется нечетким множеством с помощью функции принадлежности. Нечеткое множество характеризуется функцией принадлежности, которая позволяет вычислить степень принадлежности произвольного терм-множества (в данном примере – вероятности реализации угрозы фрода, ущерба фрода) универсальному множеству.

Таблица 1. Связь вероятности и ущерба угроз с риском ИБ

Вероятность угрозы	Ущерб от реализации угрозы				
	Незначит.	Малый	Средний	Существенный	Недопустимый
Низкая	1	1	2	3	4
Средняя	1	2	3	4	5
Высокая	2	3	4	5	5

Для каждого термина множества лингвистических переменных вероятности реализации угрозы фрода и лингвистических переменных ущерба при реализации угрозы фрода производится построение функций принадлежности термина. В основу может быть положен широко используемый метод последовательных интервалов, использующий опрос экспертов. Пример использования такого метода приведен в работе [3]. Для построения функции принадлежности определенного термина по результатам опроса экспертов составляется два графика размытости смежных с ним термов. Используя эти графики, формируется искомая функция принадлежности.

В работе [3] приведен также метод построения функций принадлежности термина для риска безопасности угрозы. Для получения значения выходной переменной риск угрозы ИБ используем алгоритм нечеткого вывода Мамдани. Определим в настоящем примере для лингвистической переменной риска безопасности угрозы фрода следующие терм-множества: низкий, умеренный, средний, высокий, экстремальный.

## 1.2. Фазификация

Этап фазификации заключается в применении решающих правил к входным данным (оценки экспертов вероятности и ущерба угрозы) и служит для конвертации четких входных данных к нечеткому формату. Связь входных и выходных (риск угрозы) величин представлена в таблице 1.

Из приведенного примера следует, что использование экспертного метода при выборе числа множеств в терм-множестве и формировании функций принадлежности термина является субъективным. Использование этих данных может быть причиной недостоверной оценки риска угрозы фрода, их ранжирования и как следствия принятие первоочередных мер по усилению защиты от угроз не с самым высоким уровнем риска ИБ.

Зададим продукционные правила с единичными весовыми коэффициентами, соответствующие таблице 1, следующим образом.

Функции принадлежности трех нечетких множеств (вероятности угрозы, ущерба от реализации угрозы и риска угрозы ИБ) приведены соответственно на рис.2, рис.3, рис.4 соответственно.

1. If (Вероятность is Низкая) and (Ущерб is Малый) then (Риск is Низкий) (1)
2. If (Вероятность is Низкая) and (Ущерб is Средний) then (Риск is Умеренный) (1)
3. If (Вероятность is Низкая) and (Ущерб is Существенный) then (Риск is Средний) (1)
4. If (Вероятность is Низкая) and (Ущерб is Недопустимый) then (Риск is Высокий) (1)
5. If (Вероятность is Низкая) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
6. If (Вероятность is Средняя) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
7. If (Вероятность is Средняя) and (Ущерб is Малый) then (Риск is Умеренный) (1)
8. If (Вероятность is Средняя) and (Ущерб is Средний) then (Риск is Средний) (1)
9. If (Вероятность is Средняя) and (Ущерб is Существенный) then (Риск is Высокий) (1)
10. If (Вероятность is Средняя) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)
11. If (Вероятность is Высокая) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
12. If (Вероятность is Высокая) and (Ущерб is Малый) then (Риск is Средний) (1)
13. If (Вероятность is Высокая) and (Ущерб is Средний) then (Риск is Высокий) (1)
14. If (Вероятность is Высокая) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
15. If (Вероятность is Высокая) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)

Рис. 1. Заданные продукционные правила

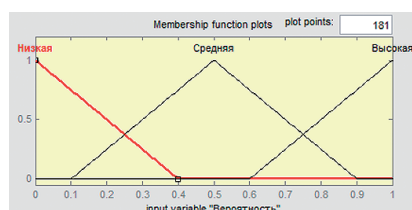


Рис. 2. Вероятность угрозы

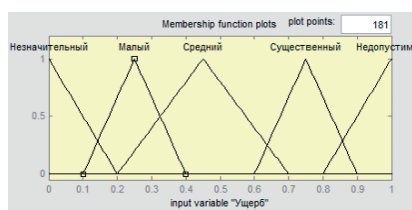


Рис. 3. Ущерб от реализации угрозы

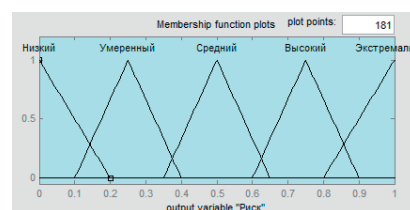


Рис. 4. Риск угрозы

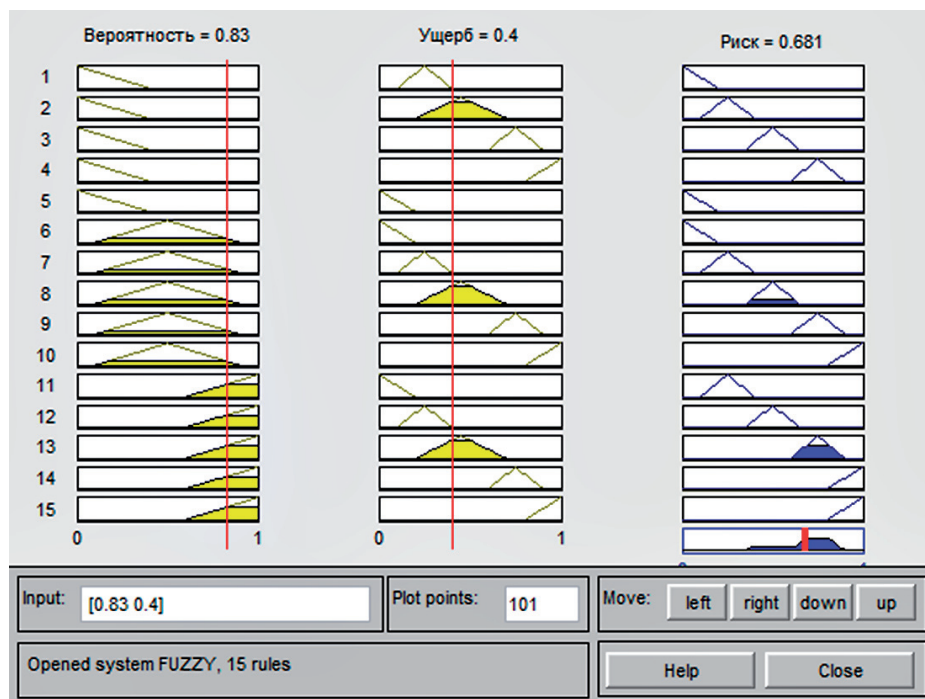


Рис. 5. Графическая интерпретация алгоритма нечеткого вывода Мамдани

### 1.3. Деагификация

Определяется четкое значение выходного значения параметра риска анализируемой угрозы фрода (например, центридным методом, как центр тяжести для кривой  $H_i(z)$ ):

$$R_0 = \frac{\int_0^1 R \mu_{\Sigma}(R) dR}{\int_0^1 \mu_{\Sigma}(R) dR} = 0.68$$

Для автоматизации процесса получения четких значений «риска информационной безопасности» по алгоритму нечеткого вывода Мамдани можно воспользоваться пакетом Fuzzy Logic Toolbox системы разработки MATLAB.

На рисунке 5 представлена графическая интерпретация алгоритма нечеткого вывода Мамдани для рассматриваемого примера угрозы ( $P=0,83$  и  $U=0,4$ ) и полученный результат риска, равный 0.681.

### 2. Уровни риска угроз фрода при различных экспертных данных

В настоящем разделе производится определение уровней риска шести угроз фрода со следующими характеристиками вероятности реализации угроз  $P$  и ущерба  $U$ :

1.  $P = 0,83$ ,  $U = 0,4$ ; 2.  $P = 0,6$ ,  $U = 0,7$ ; 3.  $P = 0,41$ ,  $U = 0,5$ ;
4.  $P = 0,2$ ,  $U = 0,61$ ; 5.  $P = 0,6$ ,  $U = 0,35$ ; 6.  $P = 0,72$ ,  $U = 0,8$ .

Для этого рассчитываются значения риска этих угроз ИБ при разных составах экспертных данных теории множественных чисел - функции принадлежности, терм-множества и продукционных правил. Расчет производится для четырех вариантов состава этих экспертных данных.

**Вариант 1.** Функции принадлежности, терм-множества и продукционные правила те же, при которых производился расчет для приведенного примера ( $P = 0,83$ ,  $U = 0,4$ ).

**Вариант 2.** Состав аналогичен варианту 1, кроме измененных функций принадлежности. На рис. 6-8 приведены эти функции принадлежности.



Рис. 6. Вероятность реализации угрозы

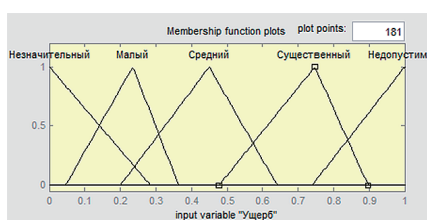


Рис. 7. Ущерб от реализации угрозы

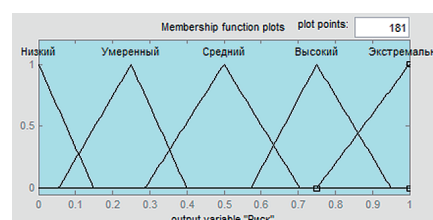


Рис. 8. Риск угрозы ИБ



Таблица 2. Связь вероятности и ущерба угроз с риском ИБ

Вероятность угрозы	Ущерб от реализации угрозы, У			
	Малый	Средний	Существенный	Недопустимый
Низкая	1	1	3	4
Средняя	1	2	3	4
Выше среднего	2	3	3	4
Высокая	2	3	4	4



Рис. 9. Вероятность реализации угрозы

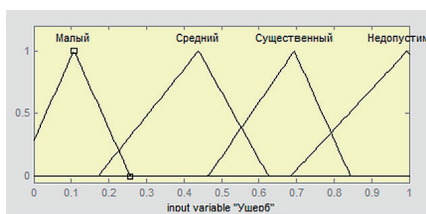


Рис. 10. Ущерб от реализации угрозы

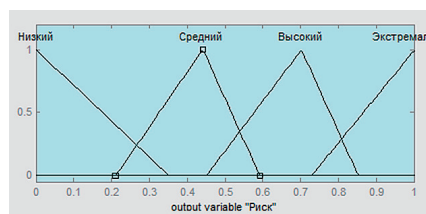


Рис. 11. Риск угрозы ИБ

**Вариант 3.** Состав аналогичен варианту 1, кроме измененных терм-множеств.

Новые терм - множества

Вероятность – Низкая, Средняя, Выше среднего, Высокая.

Ущерб- Малый, Средний, Существенный, Недопустимый.

Риск - Низкий, Средний, Высокий, Экстремальный.

Связь входных (Вероятность угрозы, Ущерб от реализации угрозы) и выходных (Риск угрозы) величин представлена в таблице 2.

На рис. 9-11 представлены новые функции принадлежности.

**Вариант 4.** Состав аналогичен варианту 1, кроме измененных продукционных правил.

В таблице 3 приведены измененные по сравнению с табл.1 экспертные данные связи вероятности и ущерба угроз с риском ИБ

В таблице 4 приведены для каждого варианта состава экспертных данных теории множеств чисел (функции принадлежности, терм-множества и продукционных правил) результаты ранжирования всех шести анализируемых угроз

Таблица 3. Связь вероятности и ущерба угроз ИБ с риском

Вероятность угрозы	Ущерб от реализации угрозы				
	Незначит.	Малый	Средний	Существенный	Недопустимый
Низкая	1	1	3	3	4
Средняя	2	2	4	5	5
Высокая	2	3	4	5	5

1. If (Вероятность is Низкая) and (Ущерб is Малый) then (Риск is Низкий) (1)
2. If (Вероятность is Низкая) and (Ущерб is Средний) then (Риск is Средний) (1)
3. If (Вероятность is Низкая) and (Ущерб is Существенный) then (Риск is Средний) (1)
4. If (Вероятность is Низкая) and (Ущерб is Недопустимый) then (Риск is Высокий) (1)
5. If (Вероятность is Низкая) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
6. If (Вероятность is Средняя) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
7. If (Вероятность is Средняя) and (Ущерб is Малый) then (Риск is Умеренный) (1)
8. If (Вероятность is Средняя) and (Ущерб is Средний) then (Риск is Высокий) (1)
9. If (Вероятность is Средняя) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
10. If (Вероятность is Средняя) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)
11. If (Вероятность is Высокая) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
12. If (Вероятность is Высокая) and (Ущерб is Малый) then (Риск is Средний) (1)
13. If (Вероятность is Высокая) and (Ущерб is Средний) then (Риск is Высокий) (1)
14. If (Вероятность is Высокая) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
15. If (Вероятность is Высокая) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)

Рис. 12. Заданные продукционные правила



Таблица 4. Ранги риска угроз ИБ для каждого варианта

Ранг риска угроз ИБ	Вариант 1	Вариант 2	Вариант 3	Вариант 4
1	$R_6(0,72;0,8) = 0,801$	$R_6(0,72;0,8) = 0,796$	$R_6(0,72;0,8) = 0,761$	$R_2(0,6;0,7) = 0,931$
2	$R_2(0,6;0,7) = 0,75$	$R_1(0,83;0,4) = 0,76$	$R_2(0,6;0,7) = 0,678$	$R_6(0,72;0,8) = 0,923$
3	$R_1(0,83;0,4) = 0,681$	$R_2(0,6;0,7) = 0,759$	$R_1(0,83;0,4) = 0,6$	$R_3(0,41;0,5) = 0,751$
4	<b><math>R_3(0,41;0,5) = 0,5</math></b>	$R_3(0,41;0,5) = 0,529$	$R_4(0,2;0,61) = 0,573$	$R_1(0,83;0,4) = 0,75$
5	$R_5(0,6;0,35) = 0,401$	$R_5(0,6;0,35) = 0,458$	$R_5(0,6;0,35) = 0,529$	$R_4(0,2;0,61) = 0,622$
6	$R_4(0,2;0,61) = 0,397$	$R_4(0,2;0,61) = 0,42$	<b><math>R_3(0,41;0,5) = 0,47</math></b>	$R_5(0,6;0,35) = 0,551$

фрода в порядке от наибольшего к наименьшему риску угрозы ИБ. Обозначим через  $R_i(P;U)$  риск  $i$ -й угрозы фрода с вероятностью реализации  $P$  и ущербом  $U$ . Тогда для угрозы, при которой производился расчет в разделе 1 статьи,  $R_1(0,83;0,4) = 0,681$ . Уровень риска угроз ИБ определяется диапазоном значений риска ИБ. Для представленных вариантов они будут разные. Поэтому ограничимся таблицей 4 рангов риска.

Из приведенных в таблице результатов для рассмотренных примеров можно отметить следующие зависимости уровня риска угроз ИБ от экспертных данных.

1. В основном, ранг риска угрозы ИБ зависит от количественных значений экспертных показателей вероятности реализации  $P$  и ущерба  $U$ . Например, к наиболее высокой по сравнению с другими угрозе 6 ( $P=0,72$ ;  $U=0,8$ ) относится наиболее высокий ранг риска в трех вариантах состава экспертных данных функции принадлежности, термножества и продукционных правил. В четвертом варианте риск этой угрозы незначительно меньше по сравнению с угрозой 2.
2. В некоторых вариантах состава экспертных данных функции принадлежности, термножества и продукционных правил уровни риска одних и тех же угроз могут существенно различаться. Например, в варианте 2 угрозе 2 соответствует третий ранг риска, а угрозе 3 – второй ранг риска. В

варианте 1 – наоборот. Исключение составляет в варианте 3, при котором угрозе 4 соответствует ранг риска 3, а угрозе 3 – ранг риска 6, а в варианте 1 – наоборот. В этом случае ранги риска ИБ угроз 3 и 4 в вариантах 1 и 3 состава экспертных данных функции принадлежности, термножества и продукционных правил отличаются на два. При этом в варианте 3 ранг риска угрозы 3 наименьший (шесть), а в варианте 1 – ранг риска этой угрозы четвертый. Если сравнивать варианты 4 и 3, то ранги риска угроз 3 и 4 отличаются еще более – на три. При этом в варианте 3 ранг риска угрозы 3 наименьший (шесть), а в варианте 4 – ранг риска этой угрозы третий.

### Выводы

Показано, что при расчете риска угрозы ИБ с помощью модели нечетких множеств с разными возможными вариантами состава экспертных данных для одних и тех же угроз уровни риска ИБ могут существенно различаться. В качестве таких данных рассматривались: функции принадлежности, термножества, продукционные правила. Это приводит к тому, что первоочередные меры по защите могут относиться к угрозам не с более высоким уровнем риска ИБ.

Расчет производился на примерах нескольких угроз фрода в сигнализации по протоколу SIP сети VoIP (сеть передача речи и данных поверх IP).

### Литература

1. Д. Рутковская, М. Пилиньский, Л. Рутковский. Нейронные сети, генетические алгоритмы и нечеткие системы. М: Горячая линия-Телеком, 2006. 388 с.
2. Maxwell Dondo. A Fuzzy Risk Calculations Approach for a Network Valnurability Ranking System. Defence R@D Canada-Ottawa, Technical Memorandum [Электронный ресурс]. 2007.

### References

1. D. Rutkovskaya, M. Pilin'skij, L. Rutkovskij. Nejrornyie seti, geneticheskie algoritmy i nechetkie sistemy. M: Goryachaya liniya-Telekom, 2006. 388 s.
2. Maxwell Dondo. A Fuzzy Risk Calculations Approach for a Network Valnurability Ranking System. Defence R@D Canada-Ottawa, Technical Memorandum [EHlektronnyj resurs]. 2007.

3. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. М: РадиоСофт, 2010. 256 с.
4. Моёров А.С., Бельфер Р.А. Общие положения и математический аппарат для определения характеристики вероятности угроз в транспортной сети VANET, Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана, 2012. С. 132-134.
5. Бельфер Р.А. Сравнительный анализ моделей оценки уровня риска угроз ИБ сети связи (по материалам ETSI). Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана, 2013. С. 12-15.
6. Sisalem D. [and others]. SIP security. N.Y. Wiley, 2009. 355 p.
7. Матвеев В.А., Морозов А.М., Р.А. Бельфер. Фрод и угрозы в сети IP-телефонии по протоколу SIP. Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение», Специальный выпуск №5, «Информатика и системы управления», 2012. С. 236-248.
8. А.М.Морозов. Анализ уязвимостей сети SIP к угрозам фрода // Электросвязь. 2013. №7. С. 10-13.
3. SHHerbakov V.B., Ermakov S.A. Bezopasnost' besprovodnykh setej: standart IEEE 802.11. M: RadioSoft, 2010. 256 s.
4. Moyorov A.S., Bel'fer R.A. Obshhie polozheniya i matematicheskij apparat dlya opredeleniya kharakteristiki veroyatnosti ugroz v transportnoj seti VANET, Sbornik trudov vserossijskoj nauchno-tekhnicheskoj konferentsii «Bezopasnye informatsionnye tekhnologii» NII RL MGTU im. N.EH.Baumana, 2012. S. 132-134.
5. Bel'fer R.A. Sravnitel'nyj analiz modelej otsenki urovnya riska ugroz IB seti svyazi (po materialam ETSI). Sbornik trudov vserossijskoj nauchno-tekhnicheskoj konferentsii «Bezopasnye informatsionnye tekhnologii» NII RL MGTU im. N.EH.Baumana, 2013. S. 12-15.
6. Sisalem D. [and others]. SIP security. N.Y. Wiley, 2009. 355 p.
7. Matveev V.A., Morozov A.M., R.A. Bel'fer. Frod i ugrozy v seti IP-telefonii po protokolu SIP. Vestnik MGTU im. N.EH. Baumana, ser. «Priborostroenie», Spetsial'nyj vypusk №5, «Informatika i sistemy upravleniya», 2012. C. 236-248.
8. A.M.Morozov. Analiz uyazvimostej seti SIP k ugrozam froda // EHlektrosvyaz'. 2013. №7. S. 10-13.

*Рецензент: Горшков Юрий Георгиевич,  
кан дидат технических наук, доцент*



# ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СРЕДАХ И ОБЛАЧНЫХ ПЛАТФОРМАХ

*Зубарев Игорь Витальевич, кандидат технических наук, доцент  
Радин Павел Константинович*

*Рассмотрены основные угрозы безопасности информации в виртуальных средах и облачных платформах. Рассмотрены проблемные вопросы защиты гипервизора, сервера управления, виртуальной машины и приложений, безопасности сетевого взаимодействия. Предложены меры по организации защиты информации в виртуальных средах и облачных платформах.*

**Ключевые слова:** облачные вычисления, виртуализация, средства защиты информации

## THE BASIC INFORMATION SECURITY THREATS IN THE VIRTUAL ENVIRONMENTS AND CLOUD PLATFORMS

*Igor Zubarev, Ph.D., Associate Professor  
Pavel Radin*

*The main threats to the security of information in virtual environments and cloud platforms are shown. Problem questions of protection of the hypervisor management server, virtual machine and application, security, networking is proposed. The arrangements for the protection of information in virtual environments and cloud platforms are considered.*

**Keywords:** cloud computing, virtualization, information security tools

### Введение

В настоящее время одним из перспективных направлений совершенствования информационно-вычислительных ресурсов является внедрение технологии облачных вычислений [1, 2].

Под облачными вычислениями (cloud computing) понимают модель обеспечения глобального и комфортного сетевого доступа по требованию к совместно используемому пулу конфигурируемых вычислительных ресурсов (например, серверам, сетям передачи данных, системам хранения данных, программным приложениям и сервисам – как совместно, так и локально), которые могут быть оперативно выделены и освоены с минимальными эксплуатационными затратами<sup>1</sup>.

Для обеспечения согласованной работы узлов вычислительной сети, реализованной на облач-

ной платформе, используется специализированное промежуточное программное обеспечение, обеспечивающее мониторинг состояния оборудования и программ, балансировку нагрузки, обеспечение ресурсов для решения задачи.

Одним из основных решений для сглаживания неравномерности нагрузки на вычислительные ресурсы является размещения слоя серверной виртуализации между слоем программных услуг и аппаратным обеспечением. В условиях виртуализации балансировка нагрузки может осуществляться посредством программного распределения виртуальных серверов по реальным серверам, перенос виртуальных серверов происходит посредством живой миграции.

Следует признать, что технология виртуализации имеет множество преимуществ, например: удобство управления виртуальной средой; высокая скорость разворачивания новых серверов; оперативность создания резервных копий, тестирования обновлений и нового функционала на

<sup>1</sup> NIST SP 800-145. Definition of Cloud Computing.

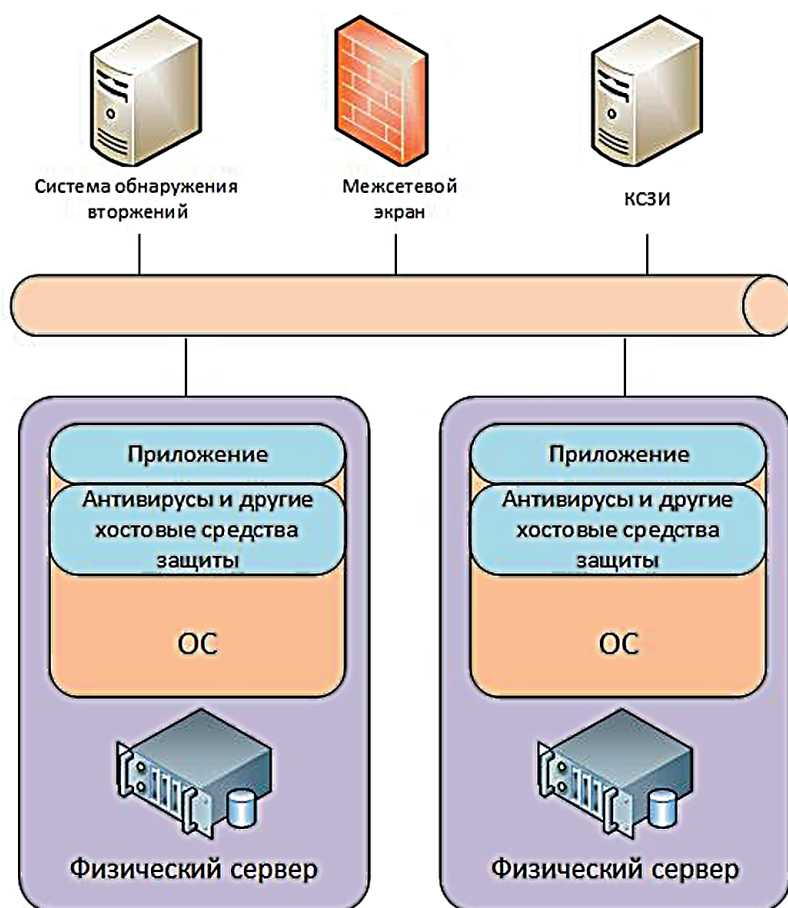


Рис. 1. Элементы физической вычислительной среды

актуальных копиях продуктивных систем и др. [3].

Однако обеспечение безопасности виртуализации необходимо рассматривать как отдельное направление в рамках общей безопасности ИТ-инфраструктуры, для которого неприменимы традиционные для физической среды средства и методы защиты [4-11].

В физической среде (рис. 1) нет ограничений на применение средств защиты на хосте: сетевой трафик может быть отфильтрован стандартным сетевым оборудованием, а злонамеренный код – обнаружен системами предотвращения вторжений и контентной фильтрации.

В виртуальной же среде (рис. 2) применение традиционных средств защиты информации иногда невозможно или нецелесообразно. Например, одновременная антивирусная проверка жестких дисков нескольких виртуальных машин создаст значительную нагрузку на оборудование. Сетевой трафик между виртуальными машинами не покидает физического сервера, и, следовательно, традиционные сетевые средства защиты информации его не видят. Кроме того, имеется дополнительный программный слой, который также необходимо защищать.

### Проблемные вопросы безопасности виртуализации

Рассмотрим «узкие» места безопасности виртуализации: гипервизор, сервер управления, виртуальные машины, приложений и др.<sup>2</sup>

**1. Гипервизор** – это программа или аппаратная схема, обеспечивающая или позволяющая одновременное параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере. Он обеспечивает изоляцию ОС друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами. В этом смысле гипервизор обозначает целый класс ПО, которое отвечает за процесс исполнения ВМ, и отделяет эту категорию продуктов от других компонентов системы виртуализационного ПО (в частности, от средств управления теми же гипервизорами и виртуальными средами)

Компрометация гипервизора может привести к компрометации всех его виртуальных машин. Автономный гипервизор (работающий непосредствен-

<sup>2</sup> См. <http://habrahabr.ru/company/securitycode/blog/200346/>

но на оборудовании) наиболее распространенных платформ виртуализации представляет собой «урезанную» версию одной из ОС общего пользования (Windows, Linux, BSD и т.д.), и, несмотря на то что здесь отключен лишний функционал и разработчики обычно заявляют о повышенной безопасности данной версии, говорить о полном отсутствии в них невыявленных уязвимостей нельзя. Помимо кода самого гипервизора, на этом уровне может быть запущен и код сторонних разработчиков: дополнения, драйверы устройств и приложения.

Рассмотрим основные классы уязвимостей гипервизоров на примере VMware vSphere.

### А. Переполнение буфера и вызов произвольного кода

Вызвать переполнение буфера и инициировать запуск произвольного кода могут определенные ошибки в гипервизоре. Ошибки могут содержаться как на стороне управления виртуальной инфраструктурой, когда их эксплуатация проводится снаружи, с правами администратора или без них, или со стороны виртуальных машин. Во втором случае возможен выход за пределы виртуальной машины и выполнение любых команд на гипервизоре.

Примеры известных уязвимостей:

CVE-2012-1516...1517, CVE-2012-2448...2450 – VMX-процесс уязвим из-за ошибки в обработке команд, при эксплуатации уязвимости, возможно переполнение памяти и выполнение произвольного кода на хостовой операционной системе из гостевых операционных систем.

CVE-2013-3657 – Удаленный пользователь может отправить специально сформированный пакет и вызвать переполнение буфера с запуском произвольного кода или отказом в обслуживании.

CVE-2013-1405 – Удаленный пользователь может отправить специально сформированный пакет авторизации в vSphere Server 4.0-4.1, который вызовет переполнение буфера и запуск произвольного кода.

CVE-2012-2448 – Удаленный пользователь может отправить специально сформированный NFS-пакет в vSphere Server 4.0-4.1 и вызвать переполнение буфера с запуском произвольного кода или отказом в обслуживании.

### В. Повышение прав пользователя внутри виртуальной машины

Целый класс уязвимостей гипервизора позволяет нарушить работу гостевой операционной системы виртуальной машины и повысить права пользователя в ней. В виртуальной среде такие атаки реализуются обычно через два основных направления – эксплуатация уязвимостей в

VMware Tools (набор утилит и драйверов для гостевой операционной системы) или через прямой доступ к памяти виртуальной машины через гипервизор в обход механизмов доступа гостевой операционной системы.

Примеры известных уязвимостей:

CVE-2012-1666 – уязвимость VMware Tools позволяет повысить права доступа пользователю гостевой операционной системы внутри неё с помощью заражения вредоносным кодом файла `tpfc.dll`.

CVE-2012-1518 – уязвимость, позволяющая повысить права доступа пользователю гостевой операционной системы внутри неё с помощью переполнения буфера в VMware Tools, если права доступа для директории с VMware Tools настроены неправильно.

### С. Отказ в обслуживании

Это наименее опасный в плане компрометации информации класс уязвимостей, однако, подобные уязвимости влияют на другой показатель – доступность. И их реализация негативно сказывается на качестве услуг облачного провайдера, репутацию сервиса и, в конечном итоге, на прибыли. Речь идет об ошибках гипервизора, используя которые злоумышленник может привести к отказу в обслуживании, не затрачивая при этом больших усилий. Отказ в обслуживании путем генерации большого объема мусорного трафика не рассматривается как специфичная для гипервизора угроза. Речь идет об уязвимостях, при которых один или несколько простых сетевых пакетов или команд приводят к остановке в работе гипервизора целиком или отдельных его служб. Как и в случае с переполнением памяти эти ошибки могут содержаться и во внешних интерфейсах, и во внутренних функциях виртуальных машин.

Примеры подобных уязвимостей:

CVE-2013-5970 – сервис `hostd-vmdb` может быть выведен из строя путем отправки специально подготовленного сетевого пакета.

CVE-2012-5703 – API для работы внешних служб (vSphere API) содержат ошибку, которая может вызвать падение и отказ в обслуживании службы, принимающей запросы API.

Для организации защиты на этом уровне требуется:

- разработать и формализовать процессы доступа к гипервизору и изменения конфигурации;
- максимально ограничить доступ к гипервизору по сети;
- использовать возможность запуска гипервизора с флэш-памяти или с неизменяемого раздела жесткого диска;



- следить за своевременной установкой всех обновлений. Однако у такой защиты есть два недостатка. Во-первых, существует большое множество уязвимостей, известных только узкому кругу злоумышленников, но пока неизвестных производителю и, соответственно, неучтённых им. Во-вторых, при использовании сертифицированного гипервизора его обновления запрещены, так как нарушают целостность бинарных файлов;

- регулярно проводить тесты сканерами уязвимостей;

- тщательно отслеживать перемещение образов жестких дисков, подключение внешних накопителей и передачу больших объемов данных;

- тщательно проверять сторонний код и особенно контролировать физический доступ к оборудованию.

**2. Консоль/сервер управления.** Большое количество виртуальных машин, используемых в облаках требует наличие систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин — невидимок, способных блокировать одни виртуальные машины и предоставлять другие. Консоль или сервер управления (в зависимости от платформы виртуализации) — такой же программный код с доступом к его функциям по сети, следовательно, он может содержать уязвимости, которые способны привести к компрометации всех виртуальных машин. Для организации защиты на этом уровне требуется:

- управлять изменениями конфигурации (существующие средства защиты платформ виртуализации позволяют отслеживать изменения настроек и проводить их проверку на соответствие различным стандартам и/или принятым в компании политикам безопасности);

- ограничить доступ по сети (доступ только из определенных сегментов сети или размещение сервера управления в отдельном сегменте);

- обеспечить регулярное обновление;
- сканировать уязвимости;
- организовать журналирование и мониторинг.

**3. Виртуальная машина и приложения.** Стандартные средства защиты не всегда применимы для виртуальных серверов, однако развитие платформ виртуализации показывает, что этот недостаток становится еще одним преимуществом. Например, платформа VMware имеет набор интерфейсов VMsafe для взаимодействия со средствами защиты сторонних разработчиков. Для организации защиты на этом уровне требуется следующее:

- антивирусная защита. Для антивирусов, агенты которых устанавливаются на виртуальные серверы, необходимо предусмотреть расписание запуска полной проверки, чтобы избежать повышенной нагрузки на оборудование. Если платформа виртуализации предоставляет такую возможность, то наиболее эффективным средством является безагентный антивирус, который интегрируется с гипервизором и через API осуществляет проверку процессов в памяти виртуальной машины и ее дисков даже в том случае, если машина выключена. Кроме того, он позволяет избежать конкуренции за ресурсы оборудования;

- разделение виртуальных машин по зонам доверия. Возможна и допустима ситуация, когда на одном физическом сервере находятся, например, внешний сервер и компоненты ПО, реализующие функциональные задачи должностных лиц ОВУ, но при этом необходимо соблюдение как минимум тех же принципов, что и при разворачивании физических серверов. Комплексные средства защиты платформ виртуализации таких производителей, как Trend Micro, Reflex Systems, позволяют изолировать машины из разных зон доверия, а также создать профили и политики безопасности, автоматизирующие применение таких настроек. Более того, при перемещении машины на другой сервер такой профиль может предотвратить ошибочное подключение внутренней системы к внешней сети;

- своевременное выполнение обновлений ПО, периодические сканирования уязвимостей и мониторинг событий информационной безопасности;

- обновление средств защиты. Благодаря простоте включения, выключения и клонирования виртуальных серверов появление в сети машины с устаревшими антивирусными базами и обновлениями происходит гораздо чаще, чем для физических серверов. При использовании средств защиты, которые интегрируются с гипервизором, вероятность компрометации виртуальной машины минимальна.

**4. Сетевое взаимодействие.** Очень часто не учитывают тот факт, что сетевой трафик между виртуальными машинами, находящимися на одном сервере, не покидает этого сервера, и предполагают, что систем фильтрации и предотвращения вторжений до платформы виртуализации достаточно, чтобы защитить все виртуальные серверы. Предположим, что диверсионная группа получила доступ к одному из виртуальных серверов и это осталось незамеченным средствами защиты, стоящими на периметре платформы виртуализации, например они использовали одну из техноло-

гий туннелирования или раздобыли легитимный доступ к одному из серверов. Результатом могут стать атаки на соседние виртуальные серверы, и такие атаки могут быть не обнаружены. Организация защиты на этом уровне складывается из нескольких составляющих.

- Защита сетевой среды платформы виртуализации не слабее, чем устанавливается для физической среды. Наиболее эффективным средством являются виртуальные модули (Virtual Appliance) систем предотвращения вторжений и межсетевого экранирования. Такие модули могут быть частью комплексного средства обеспечения безопасности платформы виртуализации или поставляться отдельно производителями сетевых средств защиты (Juniper, Check Point и др.).

- Изоляция виртуальных машин, относящихся к разным зонам доверия.

- Сетевая защита периметра платформы виртуализации. Эта мера, хотя и является недостаточной для обеспечения безопасности, но остается необходимой. Нужно учитывать объемы трафика на этом участке сети – выбранное средство защиты должно обеспечивать соответствующую пропускную способность.

**5. Административные привилегии.** Достаточно часто внедрение платформы виртуализации на стадиях планирования и разработки архитектуры начинаются без привлечения специалистов по информационной безопасности. В результате нередко встречаются ситуации, когда подразделения службы защиты государственной тайны не могут обеспечить защиту развернутых систем. Еще один риск – нарушение принципа разделения полномочий; например, клонирование, копирование и другие манипуляции с виртуальными машинами, содержащими продуктивные данные, проводящиеся без согласований и даже уведомления данных служб. Значит, велика вероятность утечки информации, содержащей сведения, составляющие государственную тайну. Для организации защиты на этом уровне требуется к проектам по внедрению системы виртуализации привлекать специалистов по информационной безопасности, а требования по защите виртуальной инфраструктуры обязательно включать в техническое задание на разрабатываемые образцы.

Также необходимо реализовать разделение полномочий при доступе к административным функциям. Здесь первоочередная задача – понимание и формализация того, кто и за управление какими рисками несет ответственность; например, управление сетевой инфраструктурой плат-

формы виртуализации должно осуществляться подразделением, отвечающим за физические сети. Это справедливо и применительно к средствам защиты, установки обновлений, проведению аудита настроек на соответствие стандартам и политикам безопасности и т. д. Комплексные средства защиты виртуальных сред позволяют реализовать ролевое управление административными функциями и тем самым минимизировать вероятность предоставления избыточных привилегий.

### **6. Аудит и отчетность.**

В общем случае аудит настроек и анализ логов платформы виртуализации становятся еще одной задачей администраторов платформы виртуализации, и здесь главная рекомендация – соблюдать те же принципы разделения полномочий, что и для физической среды. Диверсант с административным доступом к серверу управления при недостаточном контроле настроек и журнальных файлов практически не ограничен в действиях. Для организации защиты на этом уровне требуется осуществлять анализ настроек платформы виртуализации на соответствие принятым политикам безопасности. Кроме того, необходимо проводить мониторинг событий информационной безопасности и корреляцию событий для выявления потенциально опасных действий и, безусловно, учитывать, что проблемы с производительностью платформы виртуализации затронут все работающие на ней системы, поэтому анализ загруженности виртуальных машин и всей платформы в целом необходим для обеспечения ее непрерывной работы – это позволит своевременно обнаружить и устранить «узкие» места оборудования и ПО, создающее чрезмерную нагрузку [12].

### **Заключение**

Таким образом, исходя из количества приложений и компонентов, которые должны быть защищены, к управлению защитой платформы виртуализации нужно подходить комплексно – неполная защита на одном из уровней может сделать бессмысленным использование всех остальных средств. Платформы виртуализации очень уязвимы с точки зрения безопасности и, помимо стандартных потенциально опасных мест, имеют и свои. «Точечное внедрение» средств защиты не принесет положительных результатов – количество компонентов, защиту которых нужно обеспечить, слишком велико, а риски при компрометации всей платформы слишком значительны.

## Литература

## References

1. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С.10-16.
2. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61-64.
3. Krutz R.L., Vines R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010. 384 p.
4. Беккер М.Я., Гатчин Ю.А., Кармановский Н.С., Терентьев А.О., Федоров Д.Ю. Информационная безопасность при облачных вычислениях: проблемы и перспективы // Научно-технический вестник информационных технологий, механики и оптики. 2011. № 1 (71). С. 97-102.
5. Богданов В.В., Новоселова Ю.С. Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1-2. С. 78-82.
6. Гюнтер Е.С., Нарутта Н.Н., Шахов В.Г. «Облачные» вычисления и проблемы их безопасности // Омский научный вестник. 2013. № 2-120. С. 278-282.
7. Демурчев Н.Г., Ищенко С.О. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Информационное противодействие угрозам терроризма. 2009. № 13. С. 147-151.
8. Иванов А.П., Андреев В.М., Тикин М.С. Информационная безопасность облачных вычислений // Информация и безопасность. 2012. Т. 15. № 3. С. 435-436.
9. Каретников А.В., Зегжда Д.П. Безопасность облачных вычислений. проблемы и перспективы // Проблемы информационной безопасности. Компьютерные системы. 2011. № 4. С. 7-15.
10. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35.
11. Сергеев Ю.К. Анализ угроз безопасности виртуальных информационных систем // Вестник Российского государственного гуманитарного университета. 2011. № 13. С. 160-170.
12. Уязвимости гипервизора – угроза виртуальной инфраструктуре и облаку. Блок «Код Безопасности». URL: <http://habrahabr.ru/company/securitycode/blog/200346/> (Дата обращения: 9.05.2014).
1. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti, 2013, No 1(1), pp.10-16.
2. Matveyev V.A., Tsirlov V.L. Sostoyaniye i perspektivy razvitiya industrii informatsionnoy bezopasnosti Rossiyskoy Federatsii v 2014 g, Voprosy kiberbezopasnosti, 2013, No 1(1), pp.61-64.
3. Krutz R.L., Vines R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, 2010, 384 p.
4. Bekker M.Ya., Gatchin Yu.A., Karmanovskiy N.S., Terentyev A.O., Fedorov D.Yu. Informatsionnaya bezopasnost pri oblachnykh vychisleniyakh: problemy i perspektivy, Nauchno-tehnicheskyy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki, 2011, No 1 (71), pp. 97-102.
5. Bogdanov V.V., Novoselova Yu.S. Aktualnost obespecheniya informatsionnoy bezopasnosti v sistemakh oblachnykh vychisleniy, analiz istochnikov ugroz, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, 2012, No 1-2, pp. 78-82.
6. Gyunter Ye.S., Narutta N.N., Shakhov V.G. «Oblachnyye» vychisleniya i problemy ikh bezopasnosti, Omskiy nauchnyy vestnik, 2013, No 2-120, pp. 278-282.
7. Demurchev N.G., Ishchenko S.O. Problemy obespecheniya informatsionnoy bezopasnosti pri perekhode na oblachnyye vychisleniya, Informatsionnoye protivodeystviye ugrozam terrorizma, 2009, No 13, pp. 147-151.
8. Ivanov A.P., Andreyev V.M., Tikin M.S. Informatsionnaya bezopasnost oblachnykh vychisleniy, Informatsiya i bezopasnost, 2012, Vol. 15, No 3, pp. 435-436.
9. Karetnikov A.V., Zegzhda D.P. Bezopasnost oblachnykh vychisleniy. problemy i perspektivy, Problemy informatsionnoy bezopasnosti. Kompyuternyye sistemy, 2011, No 4, pp. 7-15.
10. Markov A.S., Tsirlov V.L. Rukovodyashchiye ukazaniya po kiberbezopasnosti v kontekste ISO 27032, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 28-35.
11. Sergeyev Yu.K. Analiz ugroz bezopasnosti virtualnykh informatsionnykh sistem, Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta, 2011, No 13, pp. 160-170.
12. Uyazvimosti gipervizora – ugroza virtualnoy infrastrukture i oblaku. Blok «Kod Bezopasnosti». URL: <http://habrahabr.ru/company/securitycode/blog/200346/>



# КИБЕРБЕЗОПАСНОСТЬ И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

## Часть 2

*Карцхия Александр Амиранович, кандидат юридических наук, профессор*

В части 2 цикла статей, посвященных вопросам кибербезопасности интеллектуальной собственности и защите прав на результаты интеллектуальной деятельности и приравненных к ним средств индивидуализации юридических лиц, товаров, работ и услуг в киберпространстве, рассматривается значение интеллектуальной собственности в структуре кибербезопасности, а также особенности защиты прав интеллектуальной собственности от киберугроз.

**Ключевые слова:** интеллектуальная собственность, защита интеллектуальной собственности от киберугроз, права на результаты интеллектуальной деятельности, промышленная собственность.

## CYBERSECURITY AND INTELLECTUAL PROPERTY

### Part 2

*Alexsandr Kartskhiya, Ph.D. (Jur.Sci), Professor*

In part 2 of the series of articles devoted to the problems of cybersecurity and the protection of intellectual property rights to the results of intellectual activity and means of individualization of legal persons, goods, works and services in cyberspace, as well as discusses the importance of intellectual property in the structure of cybersecurity, especially intellectual property rights protection against cyberthreats.

**Keywords:** intellectual property, intellectual property protection against cyberthreats, rights to the results of intellectual activity, industrial property.

Интенсификация процесса мировой глобализации в значительной степени порождается развитием информационно-коммуникационных технологий и Интернета, которые в свою очередь стали основным инструментом глобальной коммуникации. Сфера интеллектуальной собственности оказалась глубоко интегрирована в глобальные процессы, которые выявили новые риски и поставили новые вопросы, связанные с защитой прав интеллектуальной собственности, обеспечением публичных (национальных) и частных (коммерческих) интересов правообладателей, созданием эффективной защиты интеллектуальной собственности в киберпространстве, сохранности государственной, служебной и коммерческой тайны.

Современные инновации, связанные с бурным развитием информационно-коммуникационных технологий, интернета, генной инженерии, биотехнологий и фармацевтики стимулируют появление новых концептуальных подходов в вопросах

интеллектуальной собственности. Приобретают особую актуальность проблемы эффективности охраны интеллектуальной собственности и защиты интеллектуальных прав, а также совершенствования правового режима охраны инноваций (изобретений и других патентоспособных объектов, авторских произведений, программ для ЭВМ и др.) при условии соблюдения рационального баланса интересов правообладателей и общества, доступности результатов новых разработок и технических решений в интересах научно-технического, социального и общекультурного развития общества [1].

Анализ концептуальных подходов и национальных стратегий развития интеллектуальной собственности в России и зарубежных странах, а также целенаправленность стратегий кибербезопасности позволяют сделать определенные выводы. Учитывая возрастающее соперничество стран в глобальной экономике и усиление конкуренции на всех уровнях, России необходимо



иметь собственную стратегию кибербезопасности, определяющую приоритеты государственной политики в этой области на ближайшую перспективу и место страны в глобальном информационном пространстве. Среди основных вопросов этот документ должен определять направления государственной политики в отношении охраны интеллектуальной собственности, использовании инструментов поощрения и защиты прав интеллектуальной собственности в целях безопасности информационно-коммуникационной среды, включая защиту интересов российских правообладателей за рубежом в глобальной информационно-коммуникационной среде. В этом отношении важно поддержать инициативу по разработке концепции стратегии кибербезопасности Российской Федерации с учетом опыта разработки проекта федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который предусматривал организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры России.

### *Интеллектуальная собственность в структуре кибербезопасности*

Правовой институт интеллектуальной собственности занимает одно из ключевых мест в законодательстве России. Результаты интеллектуальной деятельности и средства индивидуализации товаров, работ, услуг и юридических лиц, которым в силу закона предоставляется правовая охрана и которые определяются как интеллектуальная собственность в ст.1225 Гражданского кодекса РФ, представляют собой нематериальные активы, обладающие материальной, товарной стоимостью. Патенты на изобретения, полезные модели, промышленные образцы, товарные знаки, программы для ЭВМ и авторские произведения, секреты производства (ноу-хау) и другие интеллектуальные нематериальные активы, содержащие новаторские технические и гуманитарные знания и умения, в условиях глобальных рыночных отношений приобретают особую ценность для их правообладателей.

Информация (сведения) о характере и содержании новаторских достижений имеет важнейшее значение в современной высоко конкурентной среде. Независимо от того, является ли содержание таких нематериальных активов доступным неограниченному кругу лиц (описание изобретения в патенте, условное обозначение как товарный знак, обнародованное авторское произве-

дение), или сведения о передовых разработках и технологиях «скрыты» коммерческой тайной (ноу-хау) или охраняются государственной тайной, закон предоставляет защиту прав на такие нематериальные активы их правообладателям. Использование же патентов, товарных знаков, программ для ЭВМ и других объектов интеллектуальной собственности в гражданском, товарном обороте допускается с соблюдением исключительного права его законного обладателя. Формы такого использования очень разнообразны и включают как непосредственное применение, так и использование результатов интеллектуальной деятельности и средств индивидуализации в товарах, выводимых на рынки или иным образом включаемых в гражданский оборот.

Кибербезопасность, т.е. безопасность в сфере глобального Интернета и других цифровых информационно-коммуникационных сетях, тесно связана с решением задач и достижением целей, поставленных в Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) (далее - Доктрина). Те виды угроз, которые обозначены в Доктрине, в большинстве своем могут быть отнесены и к угрозам в сфере кибербезопасности с учетом особенностей киберпространства. При этом, следует учесть, что в число основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни Доктриной включены и объекты интеллектуальной собственности.

В предложенном в начале 2014 года Проекте Стратегии кибербезопасности Российской Федерации (далее – Стратегия), содержатся ряд терминологических определений, включая следующие: «информационная безопасность» - состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве; «киберпространство» - сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства); «кибербезопасность» – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

С точки зрения автора настоящей статьи Стра-



тегия также должна включать положения об эффективной защите передовых научно-технических достижений и авторских разработок с позиции применения и совершенствования правового механизма защиты прав интеллектуальной собственности (прав на результаты интеллектуальной деятельности). Совершенствование этого механизма должно преследовать цель максимальной защите интересов правообладателей, также как и соблюдение баланса публичного (общественного) интереса и частного интереса правообладателей в отношении охраняемых законом результатов интеллектуальной деятельности (изобретения, промышленные образцы, программы для ЭВМ и базы данных, селекционные достижения, секреты производства (ноу-хау), передовые авторские научно-технические разработки и др.), которые могут обладать как большой интеллектуальной значимостью, так и высокой коммерческой ценностью.

В этом аспекте под кибербезопасностью возможно понимать готовность к защите интересов правообладателей интеллектуальной собственности от имеющихся и потенциальных киберугроз.

### *Киберугрозы и права интеллектуальной собственности*

Киберугрозы в отношении интеллектуальной собственности связаны с риском нарушения интеллектуальных прав на объекты интеллектуальной собственности. Риск, как определенная вероятность наступления неблагоприятных последствий, выражается применительно к интеллектуальной собственности в возможности (с той или иной степенью вероятности) нарушения интеллектуальных прав (прежде всего, исключительного права). Нарушение прав интеллектуальной собственности заключается в неправомерном использовании результата интеллектуальной деятельности или средства индивидуализации, влекущее причинение ущерба правообладателю в форме неполученного дохода или репутационных (имиджевых) потерь. Нарушение прав интеллектуальной собственности может выражаться в непосредственном использовании, к примеру, запатентованных технических решений при производстве продукта или с использованием запатентованного способа. Косвенное нарушение прав интеллектуальной собственности происходит при импорте или ином введении в гражданский оборот контрафактной продукции (товаров).

Эффективность защиты прав интеллектуальной собственности в цифровом пространстве Интернета определяется возможностью противостоять таким нарушениям и угрозам их наступления. Угрозы нарушения прав интеллектуальной собственности в киберпространстве (киберугрозы) связаны с определенными рисками и могут оказывать влияние на само существование объекта интеллектуальных прав. В частности, в результате кибератак могут быть изменены или полностью утрачены базы данных, содержащих определенную коммерчески ценную информацию, либо могут быть разглашены сведения, содержащие коммерческую тайну, что влечет утрату конфиденциальности и прекращение права на секреты производства (ноу-хау) в соответствии со ст. 1467 ГК РФ.

Киберугрозы нарушения прав интеллектуальной собственности в сфере цифрового пространства Интернет, имеют свою специфику. В частности, к видам нарушений прав интеллектуальной собственности в киберпространстве с использованием электронно-цифровых средств можно отнести:

- незаконный доступ, получение и раскрытие сведений, составляющих коммерческие секреты (ноу-хау) служебную или государственную тайну, включая преднамеренные действия («хакерские атаки»);
- несанкционированное вмешательство в базы данных, создание и применение компьютерных программных средств для изменения или блокировки сведений в составе баз данных и иной цифровой информации (сведений);
- распространение в сети Интернет ложной (недоверенной) информации о физическом или юридическом лице либо иное нарушение права на частную жизнь или ущемление деловой репутации;
- нарушение права авторства и иных авторских и смежных прав на авторские произведения в киберпространстве;
- незаконное использование товарных знаков, наименований юридических лиц и других средств индивидуализации, включая незаконное использование обозначений в доменных именах или в контенте web-сайтов;
- преднамеренное незаконное использование средств индивидуализации (коммерческих обозначений, фирменных наименований, товарных знаков, географических обозначений) для нанесения прямого или косвенного ущерба правообладателю.

Следует при этом иметь в виду, что в силу закона правообладателем патентов, товарных зна-

ков, ноу-хау, топологий интегральных микросхем, программ ЭВМ, авторских произведений и иных объектов интеллектуальной собственности могут быть как частные лица и организации, так и Российская Федерация, субъекты РФ и муниципальные образования. В связи с этим, защита интеллектуальной собственности от киберугроз, обеспечивается не только в отношении правообладателей, обладающих различным правовым статусом, но подразделяется в зависимости от уровня защиты. Каждый уровень защиты может иметь свой правовой режим защиты, который должен обеспечивать необходимую защиту интересов правообладателя интеллектуальной собственности.

В частности, особые режимы защиты интеллектуальной собственности от киберугроз предполагает установление режима государственной тайны, а также служебной или коммерческой тайны, которые основаны на нормах федеральных законов: Закон РФ от 21.07.1993 №5485-1 (в ред. от 21.12.2013) «О государственной тайне», Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 11.07.2011г.) «О коммерческой тайне». Сохранение коммерческой, служебной и иной охраняемой законом тайны предусмотрено и другими законами, в частности: ст.9 Федерального закона от 27.07.2006 №149-ФЗ (в ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации», ст.26 Федерального закона от 26.07.2006 №135-ФЗ (ред. от 28.12.2013) «О защите конкуренции» и др.

Защита сведений об охраняемых результатах интеллектуальной деятельности, составляющих государственную или коммерческую тайну, в специальном правовом режиме предусматривается также нормами части 4 Гражданского кодекса РФ. К таким охраняемым объектам прав интеллектуальной собственности относятся, в частности, программы для ЭВМ и базы данных, в которых содержатся сведения, составляющие государственную тайну (ст.1262 ГК РФ); секретные изобретения (ст. 1349 ГК РФ) и промышленные образцы (1390 ГК РФ), содержащие сведения, составляющие государственную тайну; топологии интегральных микросхем, содержащие сведения, составляющие государственную тайну (ст.1452 ГК РФ), а также охрана секретов производства (ноу-хау), основанный на введении режима конфиденциальности, включая режим коммерческой тайны (ст. 1465 ГК РФ).

Специальный правовой режим установлен для защиты персональных данных в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 23.07.2013) «О персональных

данных» и постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и изданным в его исполнение приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 18.02.2013г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

### *Интеллектуальная собственность и новые угрозы в киберпространстве*

Задачи повышения эффективности защиты интеллектуальной собственности от новых киберугроз связаны с расширением разнообразия самих объектов ИС. Проблемы защиты доменных имен различного уровня и товарных знаков, глобализация интернет-торговли и иных услуг в сети Интернет (включая электронную биржу интеллектуальной собственности) и связанный с этим оборот контрафактной продукции, распространение «виртуальных» денег и интернет-валют, расширение возможностей 3D-принтинга, существенной повышение требований к кибербезопасности персональных данных и информационных баз данных, защита авторских прав и прав личности в интернете (включая право авторства, право на «личный имидж» или «личные бренды») - эти и другие новые факторы влекут за собой необходимость совершенствования механизма защиты в киберпространстве. Новые вызовы времени требуют новых подходов и адекватных ответов.

Современное законодательство пополняется новыми законодательными нормами, повышающими эффективность защиты интеллектуальной собственности в киберпространстве. В конце 2013 года в Гражданский кодекс РФ введены нормы об ответственности интернет-операторов (информационных посредников), которые обязаны соблюдать права обладателей интеллектуальной собственности и теперь несут самостоятельную ответственность за нарушение этих прав (ст.1253.1 ГК РФ). Информационный посредник, осуществляющий передачу материала в информационно-телекоммуникационной сети, несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных Гражданским кодексом РФ при наличии вины с учетом некоторых особенностей.

К информационному посреднику в судебном порядке могут быть предъявлены требования о защите интеллектуальных прав, не связанные с применением мер гражданско-правовой ответственности, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней.

Кроме того, эти правила об ответственности применяются в отношении лиц, предоставляющих возможность доступа к материалу или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети. В частности, правонарушителю суд может запретить размещать информацию, необходимую для получения с использованием сети «Интернет» видеофильмов на сайте информационно-телекоммуникационной сети «Интернет» без согласия правообладателя или иного основания, предусмотренного Гражданским кодексом РФ.

В Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации» установлены правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Предусмотрен порядок ограничения доступа в информационно-комму-

никационных сетях (включая Интернет) к информации, распространяемой с нарушением закона, в которой содержатся призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях.

Значение защиты ценных технологий и информации от кражи, шпионажа или других методов незаконного присвоения возрастает в силу факторов глобализации, использования аутсорсинга, удлинения цепочки поставок товаров, широкого использования информационно-коммуникационных технологий и т.д.), Увеличиваются риски того, что украденная коммерческая информация (trade secrets) будет использоваться в третьих странах для производства контрафактных товаров [2].

Серьезную озабоченность вызывают угрозы бизнесу от промышленного шпионажа в пользу конкурентов и экономического шпионажа в пользу иностранных государств. Особое значение приобретает сохранность и защита коммерческой информации (коммерческих секретов), которыми обладают работники при выполнении своих трудовых функций. О вопросах защиты коммерческих секретов и иных средств индивидуализации пойдет речь в следующей части цикла статей.

### Литература

1. Карцхия А.А. Права промышленной собственности в российском праве: навстречу вызовам современности. Lambert Academic Publishing. Germany, 2013.
2. EU Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure <http://ec.europa.eu/>

### References

1. Kartskhiya A.A. Industrial property rights in the Russian law: towards challenges. Lambert Academic Publishing. Germany, 2013.
2. EU Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure <http://ec.europa.eu/>



# СИСТЕМАТИЗАЦИЯ ВИДОВ ОТНОШЕНИЙ И ОТВЕТСТВЕННОСТИ ПРИ ПОЛУЧЕНИИ ДОСТУПА К ИНФОРМАЦИИ

**Федичев Андрей Валерьевич**, кандидат технических наук, доцент  
**Артамошин Сергей Александрович**

Рассматривается правовое регулирование отношений в сфере информационных технологий. Систематизированы виды отношений и виды ответственности и представлены в виде исчерпывающих таблиц. Рассмотрены условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации.

**Ключевые слова:** защита информации, служебная тайна, неприкосновенность частной жизни, ответственность за разглашение.

## A SYSTEMATISATION OF TYPES OF RELATIONSHIPS AND RESPONSIBILITY IN ACQUIRING ACCESS TO INFORMATION

**Andrey V. Fedichev, Ph.D., Associate Professor**  
**Sergey A. Artamoshin**

Legal regulation of relationships in the sphere of information technologies is considered. Types of these relationships and responsibility are systematised and presented in the form of comprehensive tables. Conditions of classifying information as a commercial secret, official secret, or confidential information of any other kind, and the obligation to comply with the confidentiality of such information are considered.

**Keywords:** information protection, official secret, inviolability of private life, liability for disclosure of information.

«Цзылу сказал Конфуцию: «Правитель Вэя предлагает доверить Вам правительство. Как Вы считаете, что надо будет сделать прежде всего? Главное – сделать верными наименования.» - Ответил Конфуций. И добавил «Если наименования неточны, слова не будут подходить; если слова не подходят, государственные дела придут в упадок; если эти дела не будут иметь успеха, если ни обряды, ни музыка не процветают, кары и наказания не могут применяться справедливо; если они не применяются справедливо, народ не будет знать, как действовать. Поэтому мудрец, распределяя наименования, всегда действует таким образом, чтобы слова им точно соответствовали, а употребляя их в разговоре, он опять же действует так, чтобы эти слова проявлялись в поступках. Пусть мудрец не допускает ни малейшего легкомыслия в своих словах! Этого достаточно». Louen yu, L, p. 187; SMT, V, p. 378

Центральным понятием законодательства «об информации, информационных технологиях и о защите информации» является понятие «информация». В ранее действовавшем Законе «Об информации, информатизации и защите информации» от 1995 г. под информацией понимались сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления. В новом Федеральном законе «Об информации, информационных технологиях и о защите информации» определение информации представлено в более общем виде. Информацией являются любые сведения (сообщения, данные) независимо от формы их предоставления.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, согласно Закону «Об информации, информационных технологиях и о защите информации» основывается на следующих принципах:



1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) **установление ограничений доступа к информации только федеральными законами;**

3) **открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;**

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) **неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;**

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 9 Закона «Об информации, информационных технологиях и о защите информации» в рамках реализации принципов изложенных в п.2 и п.3 («Ограничение доступа к информации») установила:

1. Ограничение доступа к информации **устанавливается федеральными законами** в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой **ограничен федеральными законами.**

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. **Федеральными законами** устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Для того, чтобы более детально разобраться в сложившейся ситуации, подробно рассмотрим построение системы законодательства. Итак, под системой законодательства понимается совокупность действующих на территории данного государства нормативно-правовых актов. При этом под нормативно-правовым актом понимается официальный документ компетентного государственного органа, направленный на возникновение, изменение или отмену норм права. Нормативно-правовые акты обладают как общими признаками, характеризующими все правовые акты, так и специфическими, отличающими их от иных видов правовых актов. Так, нормативно-правовые акты имеют государственно-властную природу, исходят от компетентных органов государства, существуют в форме официальных документов со всеми необходимыми атрибутами, обязательны для исполнения и поддерживаются силой государственного принуждения в случае их нарушения - в этом состоят их общие признаки как разновидности правовых актов. Кроме этого, нормативно-правовые акты направлены на возникновение, изменение или отмену норм права - в этом их специфический признак.

Основным критерием классификации нормативно-правовых актов является юридическая сила нормативного акта. Юридическая сила нормативно-правового акта - это технико-юридическая характеристика нормативно-правового акта, выражающая степень его подчиненности иным нормативным актам, его место в иерархии нормативных актов, которая зависит от места государственного органа, принявшего этот акт, в системе органов государства.

В зависимости от юридической силы все нормативно-правовые акты делятся на две группы:

1. Законы;

2. Подзаконные акты.

Закон - это принятый в особом порядке первичный нормативно-правовой акт высшего представительного органа государственной власти, обладающий высшей юридической силой и регулирующий важнейшие общественные отношения. При этом сами законы также делятся на виды в зависимости от юридической силы. Классификация законов РФ в порядке убывания юридической силы выглядит следующим образом:

1) **Конституция**

Принимая во внимание, что «Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации. Законы и иные правовые акты, принимаемые в Российской Фе-

дерации, не должны противоречить Конституции Российской Федерации» (статья 15 Конституции РФ) сформулируем основные гарантии:

**Статья 2** «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства».

**Статья 7** «Российская Федерация – социальное государство, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека».

**Статья 8** «В Российской Федерации гарантируется единство экономического пространства, свободное перемещение товаров, услуг и финансовых средств, поддержка конкуренции, свобода экономической деятельности».

**Статья 23** «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».

**Статья 24** «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

**Статья 29** «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

**Статья 34** «Каждый имеет право на свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности».

**Статья 35** «Право частной собственности охраняется законом».

**Статья 41** «Соккрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом».

**Статья 55** «Перечисление в Конституции Российской Федерации основных прав и свобод не должно толковаться как отрицание или умаление других общепризнанных прав и свобод человека и гражданина. В Российской Федерации не долж-

ны издаваться законы, отменяющие или умаляющие права и свободы человека и гражданина. **Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства».**

## **2) Федеральные конституционные законы**

Федеральные конституционные законы принимаются только по вопросам, прямо предусмотренным Конституцией. Например, федеральными конституционными законами регулируется деятельность Конституционного Суда, Верховного Суда, Высшего Арбитражного Суда, Президента, Правительства и ряд других вопросов. Конституционные законы развивают положения конституции. Они обладают высшей юридической силой по сравнению с иными законами.

## **3) Федеральные законы**

Федеральные законы составляют основную массу законодательства. Они развивают, конкретизируют общие положения, установленные Конституцией и федеральными конституционными законами. Федеральные законы подразделяются на две группы:

- кодифицированные законы (кодексы, основы законодательства);
- текущее законодательство.

Кодифицированные законодательные акты обладают преимуществом по сравнению с текущим законодательством, т.к. являются основополагающими актами в той или иной отрасли права. При противоречии норм кодекса и некодифицированного закона действуют предписания кодекса, если иное специально не оговорено.

Термин «**федеральный закон**», впервые введенный Конституцией РФ 1993 г., используется ею в двух значениях. В одних статьях он означает все виды законов, принимаемых Федеральным Собранием (например, статья 4, часть 2), то есть обычные федеральные законы, федеральные конституционные законы, законы о конституционных поправках (см. пересмотр конституции). В других случаях под федеральными законами понимается только обычный закон, то есть закон, который принимается по всем вопросам, не регулируемым по прямому предписанию Конституции федеральным конституционным законом или законом о конституционных поправках.

## **4) Законы субъектов федерации.**

Законы субъектов федерации распространяют свое действие только на территорию того

региона, законодательными органами которого они были приняты. Вопросы соотношения между собой различных видов законов оговорены в ст. 76 Конституции РФ. Коротко особенности соотношения федеральных законов и законов субъектов федерации можно выразить правилом: при противоречии федерального закона и закона субъекта федерации действует федеральный закон, если он касается вопросов, отнесенных конституцией к ведению федерации в целом, и действует закон субъекта федерации, если он касается вопросов, отнесенных к предметам ведения субъектов федерации.

**Подзаконные нормативные акты** - это принятые компетентными органами или должностными лицами государства на основании и во исполнение закона правовые акты, содержащие нормы права. Подзаконные акты призваны конкретизировать и детализировать предписания законов. Характерными признаками подзаконных актов является то, что они

- 1) принимаются на основе закона,
- 2) принимаются во исполнение закона,
- 3) не могут противоречить закону.

Классификация подзаконных актов Российской Федерации в порядке убывания юридической силы выглядит следующим образом:

- 1) указы Президента;
- 2) постановления Правительства;
- 3) акты министерств и ведомств: приказы, инструкции, положения, указания, уставы, решения коллегий и др.;
- 4) акты исполнительных органов субъектов РФ: указы Президентов (в республиках); постановления глав администраций (в иных субъектах); приказы, инструкции руководителей подразделений соответствующих администраций;
- 5) акты органов местного самоуправления;
- 6) локальные нормативно-правовые акты: акты руководителей предприятий, учреждений и организаций.

Таким образом, ограничения доступа к информации могут быть установлены только законом принятым федеральным парламентом по вопросам, отнесенным конституцией к исключительной компетенции федерации, а также к совместной компетенции федерации и ее субъектов.

Наиболее наглядно процедура доступа к информации прописана в федеральном законе «О порядке рассмотрения обращений граждан Российской Федерации» который реализует «закрепленное за ним (гражданином Российской Федерации) Конституцией Российской Федерации право на обращение в государственные

органы и органы местного самоуправления, а также устанавливается порядок рассмотрения обращений граждан государственными органами, органами местного самоуправления и должностными лицами».

Так п.6 статьи 11 федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» указывает, что «в случае, если ответ по существу поставленного в обращении вопроса не может быть дан без разглашения сведений, **составляющих государственную или иную охраняемую федеральным законом тайну**, гражданину, направившему обращение, сообщается о невозможности дать ответ по существу поставленного в нем вопроса в связи с недопустимостью разглашения указанных сведений». Таким образом, если «письменное предложение, заявление или жалоба, а также устное обращение в государственный орган, орган местного самоуправления» гражданина соответствует требованиям, изложенным в статье 7 Закона, и информация не содержит ограничения изложенного п.6 статьи 11, то ответ должен быть получен «в течение 30 дней со дня регистрации письменного обращения».

*Хань Фэйцзы пишет: «Законы следует соединять и объявлять в виде таблиц; во всех административных учреждениях нужно обязательно выставлять таблицы с законами; о них необходимо оповестить весь народ». «Закон существует, когда указы и постановления выставлены во всех административных конторах, а мысль о неизбежности наказания и кары приникла во все умы. Вознаграждение связано с уважительным соблюдением закона, а наказание – с его нарушением». Han Fei tseu, p. 38,43.*

Статья 15 Конституции Российской Федерации сформулировала следующий основной принцип - «Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора».

Учитывая направленность материала в дальнейшем, понятие информация будем рассматривать в связи с его возможностью передачи (получения) сведений (сообщения, данных) независимо от формы их представления, или напротив, запретом на ее передачу (получение) третьим лицам. Иными словами, понятие информация будем связывать с движением. При рассмотрении материала в данном контексте, возникает понятие «тайны» соответствующей информации.

Принимая во внимание ранее изложенные Конституционные гарантии, условно сформулируем ограничение оборота информации о:

1) реализации обязанности Российской Федерации по обеспечению целостности и неприкосновенности своей территории;

2) праве частной собственности охраняемой законом и соответственно о реализации своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности;

3) праве на неприкосновенность частной жизни, личной и семейной тайны.

В общем виде требования ограничения оборота информации федеральными законами по предложенной классификации сведены в таблицу.

№ по перечню условного ограничения	Наименование Федерального Закона	Содержание информации, оборот которой подлежит ограничению
1	Закон «О государственной тайне»	Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.
1	Уголовный Кодекс Российской Федерации	<b>Статья 283.</b> Разглашение государственной тайны 1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.
2	Федеральный Закон «О коммерческой тайне»	закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).
2	Федеральный Закон «Об аудиторской деятельности»	<b>Статья 8.</b> Аудиторская тайна Аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги.
2	Налоговый Кодекс Российской Федерации	<b>Статья 102.</b> Налоговая тайна 1. Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: 1) разглашенных налогоплательщиком самостоятельно или с его согласия; 2) об идентификационном номере налогоплательщика; 3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; 4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам); 5) предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности.



№ по перечню условного ограниче- ния	Наименование Федерального Закона	Содержание информации, оборот которой подлежит ограничению
2	Гражданский Кодекс Российской Федерации Часть вторая	<p><b>Статья 857.</b> Банковская тайна</p> <p>1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.</p> <p>2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.</p> <p><b>Статья 946.</b> Тайна страхования</p> <p>Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса.</p>
2	Федеральный Закон «О банках и банковской деятельности»	<p><b>Статья 26.</b> Банковская тайна</p> <p>Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.</p>
2	Федеральный Закон «О страховании вкладов физических лиц в банках Российской Федерации»	<p><b>Статья 31.</b> Служебная, коммерческая и банковская тайна</p> <p>1. Агентство вправе получать информацию, составляющую служебную, коммерческую и банковскую тайну банка, в отношении которого наступил страховой случай, необходимую для осуществления им функций, установленных настоящим Федеральным законом.</p> <p>2. Агентство обязано предоставить ставшую ему известной информацию об операциях банка, в отношении которого наступил страховой случай, по счетам и вкладам, о его финансовом состоянии, а также иную информацию, являющуюся коммерческой и банковской тайной указанного банка, по запросу суда, а также Банка России.</p> <p>3. В случае разглашения Агентством или его должностными лицами информации, составляющей служебную, коммерческую и банковскую тайну, Агентство обязано в соответствии с законодательством Российской Федерации возместить причиненные убытки лицу, права которого были нарушены.</p>
2	Уголовный Кодекс Российской Федерации	<p><b>Статья 183.</b> Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну</p> <p>1. Собираение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом -</p> <p>наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.</p>
2	Гражданский Кодекс Российской Федерации Часть третья	<p><b>Статья 1123.</b> Тайна завещания</p> <p>Нотариус, другое удостоверяющее завещание лицо, переводчик, исполнитель завещания, свидетели, а также гражданин, подписывающий завещание вместо завещателя, не вправе до открытия наследства разглашать сведения, касающиеся содержания завещания, его совершения, изменения или отмены.</p> <p>В случае нарушения тайны завещания завещатель вправе потребовать компенсацию морального вреда, а также воспользоваться другими способами защиты гражданских прав, предусмотренными настоящим Кодексом.</p>
2	Федеральный Закон «Об адвокатской деятельности и адво- катуре в Российской Федерации»	<p><b>Статья 8.</b> Адвокатская тайна</p> <p>1. Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.</p> <p>2. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.</p> <p>3. Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.</p>

## Систематизация видов отношений и ответственности...

№ по перечню условного ограниче- ния	Наименование Федерального Закона	Содержание информации, оборот которой подлежит ограничению
	Административный кодекс	<p><b>Статья 13.14.</b> Разглашение информации с ограниченным доступом Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей.</p> <p><b>Статья 14.30.</b> Нарушение установленного порядка сбора, хранения, защиты и обработки сведений, составляющих кредитную историю Нарушение бюро кредитных историй установленного порядка сбора, хранения, защиты и обработки сведений, составляющих кредитную историю, - влечет наложение административного штрафа на должностных лиц в размере от двух тысяч пятисот до пяти тысяч рублей; на юридических лиц - от десяти тысяч до двадцати тысяч рублей.</p>
3	Уголовно-процессуальный Кодекс Российской Федерации	<p><b>Статья 13.</b> Тайна переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений</p> <p>1. Ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.</p> <p>2. Наложение ареста на почтовые и телеграфные отправления и их выемка в учреждениях связи, контроль и запись телефонных и иных переговоров могут производиться только на основании судебного решения.</p>
3	Федеральный Закон «О почтовой связи»	<p><b>Статья 15.</b> Тайна связи Тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, гарантируется государством. Осмотр и вскрытие почтовых отправлений, осмотр их вложений, а также иные ограничения тайны связи допускаются только на основании судебного решения. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи.</p>
3	Федеральный Закон «О связи»	<p><b>Статья 63.</b> Тайна связи 1. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.</p> <p>2. Операторы связи обязаны обеспечить соблюдение тайны связи.</p>
3	Уголовный Кодекс Российской Федерации	<p><b>Статья 138.</b> Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений 1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.</p>
3	Гражданский Кодекс Российской Федерации часть первая	<p><b>Статья 150.</b> Нематериальные блага 1. Жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право свободного передвижения, выбора места пребывания и жительства, право на имя, право авторства, иные личные неимущественные права и другие нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом.</p>
3	Федеральный Закон «О персональных данных»	<p>Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.</p>
3	Семейный Кодекс Российской Федерации	<p><b>Статья 15.</b> Медицинское обследование лиц, вступающих в брак Результаты обследования лица, вступающего в брак, составляют медицинскую тайну и могут быть сообщены лицу, с которым оно намерено заключить брак, только с согласия лица, прошедшего обследование.</p> <p><b>Статья 139.</b> Тайна усыновления ребенка Тайна усыновления ребенка охраняется законом.</p>

№ по перечню условного ограниче- ния	Наименование Федерального Закона	Содержание информации, оборот которой подлежит ограничению
3	Федеральный Закон «Об актах гражданского состояния»	<b>Статья 47.</b> Обеспечение тайны усыновления органами записи актов гражданского состояния 1. Тайна усыновления охраняется законом. 2. Работники органов записи актов гражданского состояния не вправе без согласия усыновителей (усыновителя) сообщать какие-либо сведения об усыновлении и выдавать документы, из содержания которых видно, что усыновители (усыновитель) не являются родителями (одним из родителей) усыновленного ребенка.
3	Уголовный Кодекс Российской Федерации	<b>Статья 155.</b> Разглашение тайны усыновления (удочерения) Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений, - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
3	Основы законодательства Российской Федерации об охране здоровья граждан	<b>Статья 61.</b> Врачебная тайна Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.
3	Закон «О психиатрической помощи и гарантиях прав граждан при ее оказании»	<b>Статья 9.</b> Сохранение врачебной тайны при оказании психиатрической помощи Сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья являются врачебной тайной, охраняемой законом. Для реализации прав и законных интересов лица, страдающего психическим расстройством, по его просьбе либо по просьбе его законного представителя им могут быть предоставлены сведения о состоянии психического здоровья данного лица и об оказанной ему психиатрической помощи.
3	Федеральный Закон «О государственной дактилоскопической регистрации в Российской Федерации»	<b>Статья 12.</b> Основные требования к хранению и использованию дактилоскопической информации государственные органы, указанные в статьях 11 и 14 настоящего Федерального закона, обеспечивают сохранность сведений, составляющих дактилоскопическую информацию, в режиме служебной тайны, а их должностные лица несут уголовную и административную ответственность за нарушение правил хранения и незаконное использование этой информации.
3	Уголовный Кодекс Российской Федерации	<b>Статья 137.</b> Нарушение неприкосновенности частной жизни 1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.
3	Административный кодекс.	<b>Статья 13.11.</b> Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

*«Когда ясен принцип вознаграждений и наказаний, самый глупый понимает, что от него ждут, знать и крестьянство сохраняют свой ранг, добрые и плохие стремятся поступать как можно лучше, ибо не упущена возможность распределить таланты с учетом имен и рангов, так, чтобы высшие оказались обслужены, низшие накормлены, совокупность существ управляема, а каждая личность – воспитана ... и именно это называется Великим Миром, совершенным правлением» Tchouang tseu, L.,p. 336-337.*

Учитывая вышеизложенное, встает очевидным вопрос «А где же сама «информация для служебного пользования»?»

С 1 января 2008 года утратила силу статья 319 Гражданского Кодекса, которая в доступной форме формулировала идею защиты информации - «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности». То есть если «обладатель информации» не «принимает меры к охране» конфиденциальности информации, то и говорить о том, что информация относит-

ся к какой либо из вида тайн не придется. В качестве доказательства приведем пример. Так, в 1998 г. по ст. 283 УК был привлечен к ответственности и осужден бывший сотрудник ГРУ Генштаба Министерства обороны РФ подполковник Владимир Т., передавший своему бывшему сослуживцу по Центру космической разведки слайды с изображением городов некоторых ближневосточных стран, сделанные силами космической разведки. Сослуживец подполковника Владимира Т, распорядился слайдами по собственному усмотрению. В связи с тем, что гриф «секретно» на слайдах отсутствовал, сослуживец подполковника Владимира Т не был привлечен к уголовной ответственности.

Приведенный пример в какой-то мере может объяснить свободное хождение на рынке различных информационных баз (ГАИ, налоговой инспекции, телефонные справочники и.т.д.). Но основная идея его заключается только в одном: лицо, получающее доступ к информации, должно знать, что эта информация ограниченного распространения. И термин «Для служебного пользования» в этом случае исполняет роль «стоп-фонаря» для лица, получившего доступ к информации ограниченного распространения.

Как говорится, «назовите, как хотите», только обеспечьте защиту информации, оборот которой ограничен федеральным законом.





# КАТАЛОГ ЗАКЛАДОК АНБ (SPIGEL). ЧАСТЬ 1. ИНФРАСТРУКТУРА

*Клянчин Александр Иванович*

*Рассмотрены закладки по версии журнала Spiegel. Представлена теоретическая база программно-аппаратных закладок. Приведено описание закладок, возможность встраивания, вероятные применения. Предложены организационно-технические меры по защите компьютерных ресурсов от закладок в свете современной нормативно-методической базы.*

**Ключевые слова:** программные и аппаратные закладки, уязвимость аппаратной платформы, механизмы безопасности, кибербезопасность, кибероружие.

## THE NSA'S SPY CATALOG. PART 1. INFRASTRUCTURE

*Alexander I. Klyanchin*

*The infrastructure NSA implants (reviewed in Spiegel) are considered. The theory of the hardware and software are shown. There are descriptions, implanting features, application of the implants. The organizational and technical measures to protect the computer resources from targeted malware in light of the current regulatory basis are proposed.*

**Keyword:** software implant, hardware implant, hardware vulnerability, security controls, information security management, cybersecurity, cyber weapons.



### Введение

Информационно-коммуникационные технологии являются одной из наиболее развивающихся областей науки и технологии на ближайший период. Среди основных проблем ИКТ, требующих принятия комплексных мер, является рост киберпреступности, а также защита от применения кибероружия. Осознавая

важность защиты конфиденциальной информации, защиты государственной тайны, а также принимая во внимание миниатюризацию специальных технических средств, которые дают возможность негласного снятия информации с компьютера, необходимо принимать опережающие меры по поиску и исключению программно-аппаратных закладок в устройствах массового применения.

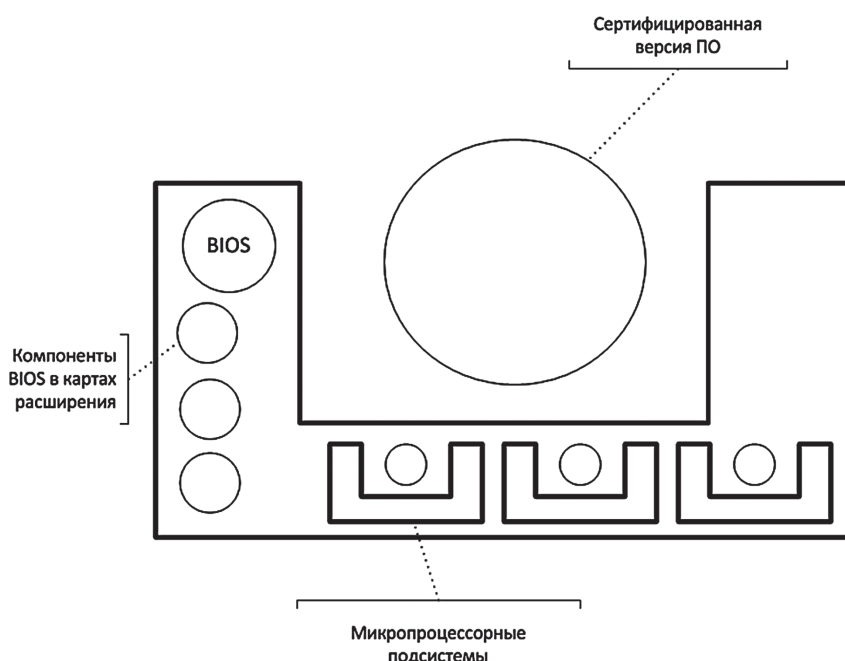


Рис. 1. Виды программного обеспечения аппаратной платформы

Код программного обеспечения выполняется центральным процессором с использованием оперативной памяти (см. Рис. 1. Виды программного обеспечения аппаратной платформы). Существует также так называемый код поддержки оборудования, который размещается в области базовой системы ввода вывода (basic input/output system - BIOS). Кроме того, в постоянном запоминающем устройстве (ПЗУ) некоторых плат расширения размещается код, который также может выполняться.

В состав аппаратных платформ входит ряд дополнительных микропроцессорных подсистем со своим кодом. Практически любая логика средней сложности реализуется с помощью микропроцессоров, ПЛИС<sup>1</sup> и т.д. Наличие потенциала по изменению функциональности только с помощью перепрограммирования отдельных

1 Программируемая логическая интегральная схема

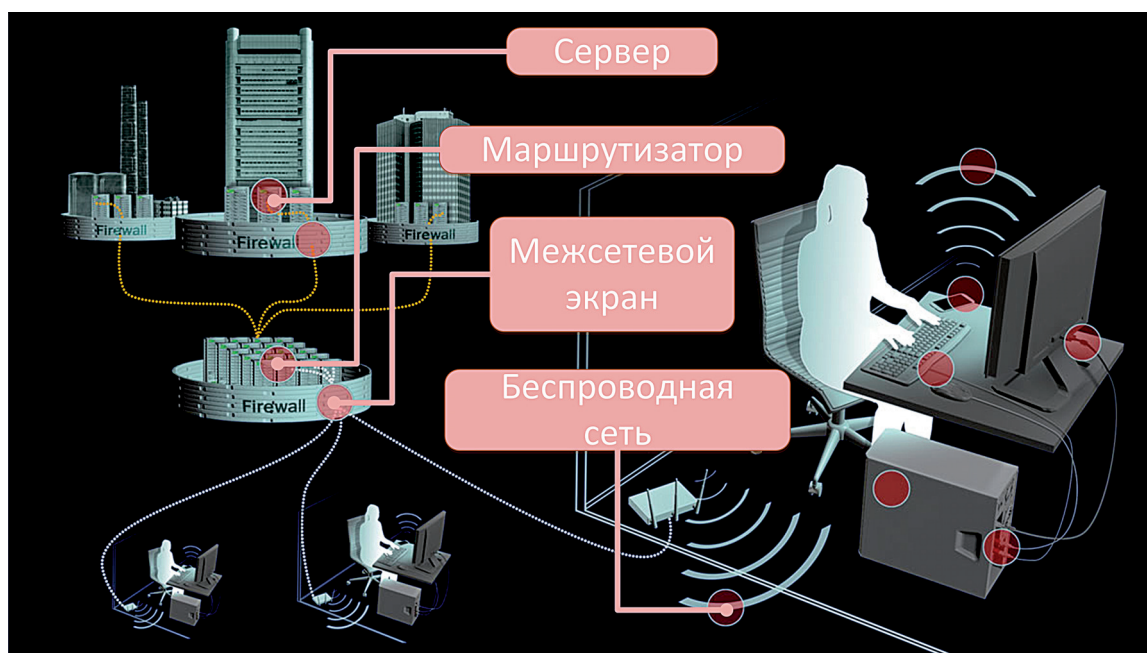


Рис. 2. Потенциальная возможность установки закладок на элементы инфраструктуры

узлов чрезвычайно расширяет возможности внедрения зловредного кода.

Зловредный код, внедренный в область BIOS, обладает следующими характеристиками:

- слабо поддается обнаружению. Как правило, это функциональный модуль, который только обеспечивает установку настоящего зловредного кода, а сам может проявляться как не декларируемая возможность или дефект;
- устойчив к перезагрузке или переустановке операционной системы;
- не подлежит контролю согласно текущей нормативной базы в системах Минобороны и ФСТЭК. На компрометированной аппаратной платформе может выполняться сертифицированный код.

Согласно 1 части каталога Spiegel практически все потенциальные закладки используют технологию внедрения в BIOS функционального модуля (импланта), который обеспечивает установку зловредного кода (см. Рис. 2. Потенциальная возможность установки закладок на элементы инфраструктуры..).

Рассмотрим список закладок по версии каталога Spiegel, которые ориентированы на инфраструктуру автоматизированной системы: межсетевые экраны, маршрутизаторы, сервера.

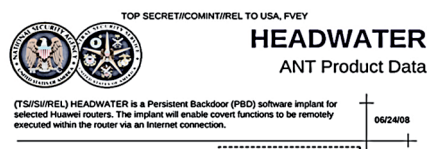
## 1. Сетевое оборудование

### 1.1. Маршрутизаторы

Маршрутизаторы - это специальные компьютеры, которые предназначены для подключения к внутренней сети компании или внешней сети, а также для передачи и обработки интернет-трафика. Согласно каталогу обзора SPIEGEL, АНТ подразделение АНБ имеет среди его предложений закладки для использования в профессиональных маршрутизаторах, выпущенных, по крайней мере, двумя производителями — **Juniper** и **Huawei**. Скорее всего, существуют дополнительные продукты подразделения АНТ для подобных устройств. Закладки, по версии каталога, устанавливаются в BIOS, на самом низком уровне программного обеспечения в каждом устройстве. Это гарантирует, что другие **дополнительные вредоносные программы** также могут быть установлены, даже если компьютер перезагружается или установлена новая операционная система. Модели маршрутизаторов, которые представлены в каталоге АНТ, предназначены для использования малого, среднего и крупного бизнеса, а также для центров обработки данных Интернет и мобильных провайдеров телефонных услуг.

#### 1.1.1. Маршрутизаторы Huawei

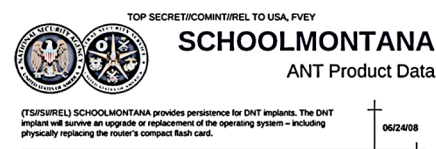
Компания Huawei (Китай) зарекомендовала себя как один из крупнейших в мире производителей сетевого оборудования. По данным исследовательской фирмы Infonetics, компания Huawei занимает **второе место** на мировом рынке во втором квартале 2013 года по продаже маршрутизаторов и коммутаторов для мобильной связи и Интернет-провайдеров, сразу за Cisco и впереди Juniper. Многие западные телекоммуникационные компании активно используют аппаратные средства Huawei, в том числе Deutsche Telekom (Германия).



**Закладка Headwater** представляет собой программную закладку для маршрутизаторов Huawei, которая обеспечивает уязвимость класса BackDoor в модуле памяти ROM. **Закладка устойчива к прошивке обновления** и предоставляет возможность **дистанционного** управления устройством. Позволяет удаленно перехватывать и анализировать все проходящие через роутер пакеты.

#### 1.1.2. Маршрутизаторы Juniper

Маршрутизаторы Juniper J – Series предназначены для соединения серверов и настольных компьютеров с корпоративной сетью и Интернетом.



**Закладка SCHOOLMONTANA** представляет собой программную закладку для устройств Juniper J Series, **устойчивую к обновлениям** программного обеспечения. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

**Маршрутизаторы Juniper M – Series** компании Juniper предназначены для организации магистральных сетей в крупных компаниях и поставщиков сетевых услуг. Они также используются в центрах обработки данных компаний, которые предоставляют другие корпорации и для частных клиентов для соединения с сетью Интернет.

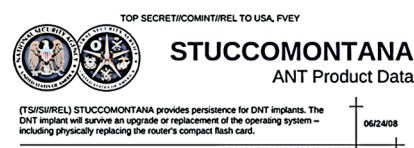


### 1.2.1. Межсетевые экраны Juniper



**Закладка SIERRAMONTANA** представляет собой программную закладку для маршрутизаторов серии Juniper M, которая **устойчива к обновлениям** прошивки и размещается в BIOS. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

**Маршрутизаторы Juniper T – Series** компании Juniper по словам производителя «используются ведущими поставщиками услуг фиксированной связи, мобильных, видео и облачных сетей».



**Закладка STUCCOMONTANA** является программной закладкой для маршрутизаторов Juniper T-Series. Существует в качестве модификации BIOS и устойчива к **обновлению программного обеспечения**. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

## 1.2. Межсетевые экраны

Аппаратные межсетевые экраны - это специальные компьютеры, которые размещаются между внутренней сетью компании или интернет - провайдера и остальной частью Интернета или разными сегментами. Они предназначены для предотвращения взлома, атак отказ в обслуживании, спама. Обеспечивают доступ терминалов сотрудников, которые регистрируются в сети компании через виртуальную частную сеть (VPN). Подразделение АНТ АНБ разработало аппаратные и программные закладки для аппаратных межсетевых экранов от основных производителей - Cisco, Juniper и Huawei - которые **превращают эти продукты** (первоначальная цель – построение защитных цифровых барьеров) **в шлюзы для поддержки атак хакеров АНБ**. Большинство закладок **размещаются в BIOS**. Это гарантирует, что закладка будет по-прежнему в активном состоянии и что вредоносные программы могут успешно закладку использовать, даже если компьютер перезагружается или проводилось обновление операционной системы.

Межсетевые экраны Juniper SSG, Netscreen G5, Netscreen 25 и 50, SSG Series предназначены для малых и средних компаний, а также филиалов крупных корпораций.



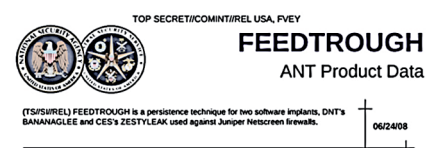
**Закладка GOURMETTROUGH** представляет собой настраиваемую программную закладку для устройств Juniper. Позволяет полностью управлять маршрутизатором, используя скрытые каналы передачи информации. Сохраняется при перезагрузке и апгрейде операционной системы маршрутизатора.

Межсетевые экраны Juniper SSG300 и SSG500 являются аппаратными брандмауэры, которые предназначены для малых и средних компаний и филиалов крупных корпораций.



**Закладка SOUFFLETROUGH** обеспечивает полный контроль над межсетевым экраном. Сохраняется при перезагрузке и апгрейде ОС. Может быть установлена удаленно если на межсетевом экране установлена другая закладка АНБ - **BANANAGLEE**.

Межсетевые экраны Juniper Netscreen / ISG 1000 являются аппаратными брандмауэры, они подходят для использования Интернет-провайдеров и операторов мобильной телефонной связи.



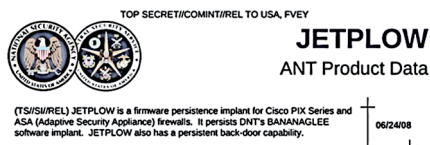
**Закладка FEEDTROUGH** позволяет обеспечивать удаленный доступ к N5XT компании, NS25, NS50, NS200, NS500, ISG1000 моделей.

### 1.2.2. Межсетевые экраны Cisco

Межсетевые экраны Cisco PIX-Series, Cisco ASA-Series. Продукты серии PIX от производителя Cisco (США) являются аппаратными межсетевыми экранами, в зависимости от модели, для малых и средних компаний, в том числе и для крупных компаний и поставщиков услуг. Производство линейки продуктов закончилась в 2008 году.



Серия ASA представляет моделью преемником PIX, и они предназначены для предприятий различных размеров, а также корпоративных центров обработки данных.



**Закладка JETFLOW:** Дает полный удаленный доступ к межсетевому экрану и трафику. Сохраняется при перезагрузке. Возможен удаленный апгрейд закладки и удаленная инсталляция если на экране стоит другая закладка АНБ **BANANAGLEE**. «Широко используется в настоящее время!». Подходит не для всех версий ОС.

### 1.2.3. Межсетевые экраны Huawei

**Межсетевые экраны серии Huawei Eudemon.** Серия Eudemon представляет собой аппаратные брандмауэры Китайского производителя Huawei и предназначены для малых и средних компаний (серии 200) и для сервис-провайдеров и крупных корпораций (1000 серии). Технология Huawei используется по всему миру в компаниях, которые включают европейские телекоммуникационные гиганты, такие как O2, Vodafone и Deutsche Telekom.



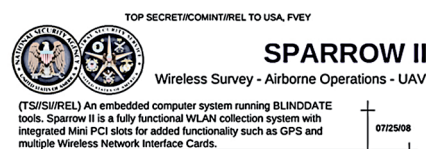
**Закладка HALLUXWATER** дает полный доступ к экрану и проходящему трафику. Остается при перезагрузке и апгрейде операционной системы (в том числе загрузочной области!). Проверена в деле.

### 1.3. Беспроводные сети

АНТ Подразделение АНБ разрабатывает методы для получения доступа к сети беспроводных сетей извне, позволяя им подключиться к этим сетям и распространять свое собственное зловерное программное обеспечение. Закладка **NIGHTSTAND**, например, может удаленно внедрить пакеты данных для различных вредоносных Windows программ. Закладка **SPARROW II**, предназначена для выявления сетей беспроводной локальной сети с воздуха. Система достаточно мала для установления на беспилотный аппарат (БЛА).



Закладка **NIGHTSTAND** представляет собой мобильную систему для беспроводной инъекции зловерного кода через уязвимости систем Windows, использующих стандарт 802.11. Согласно спецификации он работает на расстояниях до 13 километров (восемь миль).

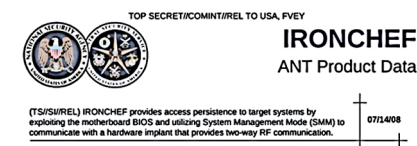


**Закладка SPARROW II** является средством выявления и составление карты беспроводных сетей, например с беспилотных аппаратов (БЛА).

## 2. Сервера

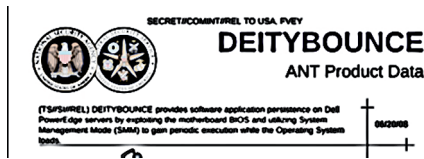
Сервера – это специальные компьютеры, которые обеспечивают доступность данных в сети компании или в сети Интернет. АНТ Подразделение АНБ разрабатывают несколько аппаратных и программных закладок для серверов производителей Dell и Hewlett-Packard. Программная закладка «DEITYBOUNCE» размещается внутри BIOS, самом низком уровне программного обеспечения, серверов Dell PowerEdge. Это расположение обеспечивает функционирование закладки по установке дополнительных шпионских программ, даже если компьютер перезагружается или осуществляется переустановка операционной системы. Предполагается, что аппаратные имплантаты для серверов Dell и HP устанавливаются на этапе доставки оборудования путем перехвата и манипулирования.

**HP DL380 G5** это сервер хранения данных пятого поколения. Он используется в корпоративных центрах обработки данных.



**Закладка IRONCHEF** основана на изменении BIOS. Закладка применяется для установления связи с АНБ инфраструктурой используя скрытые аппаратные средства. Закладка разработана для серверов семейства Proliant, которые выпускаются компанией Hewlett-Packard.

Dell PowerEdge server это сервер хранения для использования в корпоративных центрах обработки данных.



Закладка DEITYBOUNCE основана на изменении BIOS. Закладка применяется для установления связи с NSA инфраструктурой используя скрытые аппаратные средства.

### 3. Выводы

Данные, опубликованные журналом Spiegel, технологически воспроизводимы и могут являться реальной угрозой. Основным уязвимым механизмом проникновения закладок, в частности, для сетевого оборудования, является BIOS. После перепрошивки платформы становится возможным как устанавливать закладки 2-го уровня, так и обеспечивать их постоянное присутствие. Наиболее очевидным средством контроля образа BIOS является модуль доверенной загрузки. Анализ BIOS в данный момент находится на начальной

стадии и не является обязательным. Также отсутствуют простейшие способы фиксации окружения при проведении анализа на НДВ. Возможным усилением этого механизма контроля может являться единая подпись удостоверяющего центра на все BIOS, а также обязательное наличие в ПО возможность расчета и отображения контрольных сумм BIOS и ОС.

Отдельно можно отметить системный подход по покрытию целевой инфраструктуры закладками. Получается, что практически все потенциальные каналы активного взаимодействия со зловредным кодом присутствуют в каталоге – это внешние межсетевые экраны, магистральное оборудование, беспроводная связь.

Наибольший потенциал, в частности, в развитии надежного коммуникационного оборудования (маршрутизатор, межсетевой экран, поддержка беспроводных технологий), возможен на базе защищенной компонентной базы, например Эльбрус.

Имеется также предложение организации в рамках сертификации единого регистра профилей ПАК, прошедших сертификацию. Предполагается, что данный регистр должен содержать все потенциальные уязвимости аппаратной платформы и давать числовую оценку доверия.

### Литература (References)

1. Shopping for Spy Gear: Catalog Advertises NSA Toolbox. //Spiegel. <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html> .
2. Inside TAO: Documents Reveal Top NSA Hacking Unit. //Spiegel. <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html> .
3. Interactive Graphic: The NSA's Spy Catalog. //Spiegel.<http://www.spiegel.de/international/world/a-941262.html> .



# МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ РИСКАМИ

*Дорофеев Александр Владимирович, CISSP, CISA*

*Публикация продолжает серию статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional). На примере рассмотрены базовые принципы управления рисками информационной безопасности.*

**Ключевые слова:** сертификация специалистов, CISSP, система менеджмента информационной безопасности (СМИБ), управление рисками информационной безопасности.

## INFORMATION SECURITY MANAGEMENT: RISK MANAGEMENT

*Alexander Dorofeev, CISSP, CISA*

*Publication continues the series of articles devoted to preparation for the CISSP (Certified Information Systems Security Professional) exam. Basic concepts of information security risk management are examined on the real case.*

**Keywords:** experts certification, CISSP, information security management system (ISMS), risk management.

Продолжая рассматривать вопросы менеджмента информационной безопасности в настоящей статье, разберем этапы процесса *управления рисками информационной безопасности* [1, 2]. Мы будем оценивать и минимизировать риски информационной безопасности на примере, образом которого послужил реальный случай из практики.

Управление рисками информационной безопасности по своей сути является ядром системы менеджмента информационной безопасности (СМИБ). Составляющими процесса управления рисками являются процедуры своевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment) [3].

Чтобы подробно разобрать основные этапы процесса управления рисками, рассмотрим следующую ситуацию. Крупная компания-производитель стирального порошка собирается провести промо-акцию, в ходе которой должен быть развернут веб-ресурс, на котором участники акции будут регистрировать специальные коды, указанные на упаковке продукции. В качестве призов выбраны спортивные автомобили извест-

ной итальянской марки. Счастливыми обладателями дорогих автомобилей должны стать покупатели, которые регистрируют свои купоны и по счету их купоны будут соответственно 500, 10 000 или 100 000. Компания не хочет, чтобы мошенники завладели одним или несколькими призами. Нас привлекают в качестве экспертов по информационной безопасности для проведения оценки рисков и формирования рекомендаций по выбору контролей.

Чтобы не изобретать велосипед, перед созданием собственной методики оценки рисков нам стоит заглянуть в международный стандарт ISO/IEC 27001:2013 и посмотреть, какие требования к методике в нем определены.

В первую очередь стандарт требует от нас формализации процесса оценки рисков для того, чтобы применяя разработанную методику, мы могли получать сравнимые результаты.

В отличие от предыдущей версии стандарта (2005 года) в новом стандарте описание данных процессов достаточно общее. Стандартом предусмотрены лишь основные этапы оценки рисков такие как, идентификация рисков информационной безопасности, анализ рисков информаци-

онной безопасности, ранжирование рисков по степени критичности.

Исходя из практического опыта, стоит отметить, что любая хорошо продуманная методология оценки рисков информационной безопасности предусматривает такие шаги, как:

- выявление угроз, направленных на рассматриваемые активы;
- определение последствий от реализации угроз;
- выявление уязвимостей;
- выявление существующих контролей (контрмер);
- определение вероятности реализации угроз.

Как видим, шаги методики определяются, исходя из определения понятия риска. Читатели предыдущей нашей статьи, конечно, помнят, что риск определяется, как комбинация вероятности реализации угрозы и последствий. Соответствен-

но и мы будем определять релевантные угрозы, оценивать вероятность их реализации и размер ущерба.

### *Шаг 1. Определение критериев оценки*

До применения каких-либо шагов по оценке рисков, мы должны определить критерии для их оценки.

Один из подходов, позволяющих определить критерии для оценки последствий, заключается в том, чтобы оттолкнуться от целей, которые мы ставим перед информационной безопасностью. Как вы помните, защитой информации мы занимаемся для того, чтобы минимизировать финансовые потери, сохранить или даже улучшить имидж организации, а также выполнить требования регуляторов (при желании список, конечно, можно продолжить). Соответственно, и в нашем случае, мы определяем и согласовываем с заказчиком следующие уровни:

Уровень Последствий (I)	Финансовые потери	Удар по имиджу	Проблемы с регуляторами
Высокий (В)	Более 500 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию более 1 млн. чел. Например, сюжет в выпуске новостей на федеральном телеканале.	Отзыв лицензии.
Средний (С)	От 100 тыс. до 500 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию от 10 тыс. чел до 1 млн. чел. Например, публикация негативной заметки на страницах популярного блога с последующим распространением на других ресурсах.	Штраф за нарушение.
Низкий (Н)	Менее 100 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию менее 10 тыс. чел. Например, негативный отзыв на сайте организации.	Предупреждение.



## Сертификация специалистов

В случае если реализация угрозы приводит к различным видам последствий и разного уровня, то мы будем выбирать максимальный уровень.

Для оценки вероятности реализации угроз мы сознательно ограничимся следующими критериями: имеющаяся статистика по аналогичным инцидентам, требуемые затраты на реализацию угрозы и возможность обнаружения.

Важно отметить, что если бы в нашем случае речь шла не о разрабатываемой системе, а о существующей, то на вероятность реализации угрозы также влияли бы такие факторы, как наличие уязвимостей и отсутствие, либо неэффективность контролей (контрмер).

Теперь можно создать таблицу, в которой сопоставить вероятность реализации угрозы с размерами ее последствий и получить значения рисков.

Вероятность	Статистика инцидентов	Затраты на реализацию угрозы	Возможность обнаружения
Высокая (В)	Аналогичный инцидент происходит в организации каждую неделю.	<b>Финансовые затраты:</b> менее 10 тыс. руб. <b>Интеллектуальные:</b> невысокая квалификация злоумышленника. <b>Инструменты для реализации угрозы</b> общедоступны.	Угрозу и ее источник очень сложно обнаружить.
Средняя (С)	Аналогичный инцидент происходит в организации каждый месяц.	<b>Финансовые затраты:</b> от 10 тыс. до 100 тыс. рублей. <b>Интеллектуальные:</b> средняя квалификация злоумышленника. <b>Инструменты для реализации угрозы</b> можно приобрести или создать за разумный срок.	Угрозу и ее источник можно вычислить, но для этого потребуются серьезные усилия.
Низкая (Н)	Аналогичный инцидент происходит в организации каждый год.	<b>Финансовые затраты:</b> менее 100 тыс. рублей. <b>Интеллектуальные:</b> высокая квалификация злоумышленника. <b>Инструменты для реализации угрозы</b> на данный момент не доступны.	Угроза и ее источник легко обнаруживается.

Последствия Вероятность	Н	С	В
Н	Н	Н	С
С	Н	С	В
В	С	В	В

### Шаг 2. Идентификация рисков

После того, как мы определили критерии, которые мы будем использовать для оценки рисков, в соответствии с требованиями ISO 27001:2013, нам необходимо идентифицировать угрозы и, соответственно, риски.

Прежде чем бросаться в бой и формировать список рисков, проанализируем, кто или что может выступить в качестве источника угроз. В нашем случае такими источниками могут быть:

- разработчик системы,
- администратор датацентра, на площадке которого размещается веб-ресурс,
- администратор компании-организатора акции,
- внешний злоумышленник (хакер),
- недобросовестный участник акции.

Зафиксируем в следующей таблице, что плохого они могут сделать:

№	Источник угрозы	Угрозы
1	Разработчик системы	<ul style="list-style-type: none"> <li>• Внесение логической закладки. Например, как только в таблицу вносится запись под номером 499, добавляется следующая выигрышная запись с именем знакомого подставного лица.</li> <li>• Ошибки программирования, ведущие к уязвимостям системы. Например, отсутствие фильтрации данных вводимых пользователем в форму регистрации, приводящая к возможности реализации атаки SQL-инъекции</li> </ul>
2	Администратор датацентра (доступ к ОС, СУБД отсутствует)	<ul style="list-style-type: none"> <li>• Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона.</li> </ul>
3	Администратор компании-организатора акции	<ul style="list-style-type: none"> <li>• Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона.</li> <li>• Внесение в таблицу базы данных, используемых сайтом, записи с данными подставного лица.</li> </ul>
4	Внешний злоумышленник (хакер)	<ul style="list-style-type: none"> <li>• Взлом сайта. Например, для того, чтобы получить права администратора.</li> <li>• Внесение в таблицу базы данных, используемых сайтом, записи с данными подставного лица.</li> <li>• Проведение DDoS-атаки</li> </ul>
5	Недобросовестный потребитель	<ul style="list-style-type: none"> <li>• Регистрация купонов в большом количестве (нарушение условий акции).</li> </ul>

## Сертификация специалистов

Стоит отметить, что мы ограничили перечень угроз наиболее реальными (например, мы не рассматриваем угрозу падения метеорита на датацентр), также мы не спускаемся на неадекватный уровень детализации (например, отказ какой-либо микросхемы, размещенной на материнской плате сервера). Конечно, можно подобные подходы упрекнуть в том, что анализ будет не полным, но в данном случае лучше

иметь неполный анализ, чем впасть в так называемый «паралич от анализа», потратив большие ресурсы на оценку того, что никак не повлияет на ситуацию.

### Шаг 3. Оценка рисков

Теперь попробуем оценить вероятность и последствия угрозы и соответственно определить значение риска.

N	Угроза	Оценка вероятности	Комментарии к оценке	Оценка последствий	Комментарии к оценке	Риск
T1	Внесение логической закладки	C	Требуется средняя квалификация. Авторство закладки можно вычислить в виду ограниченного круга разработчиков.	B	Потеря автомобиля (ей).	B
T2	Ошибки программирования, ведущие к уязвимостям системы	H	Опытная команда разработчиков, аналогичные инциденты с данной командой происходят не чаще одного раза в год	B	Потеря автомобиля в случае, если внесенная уязвимость действительно опасная	C
T3	Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона	B	Доступны свободно-распространяемые средства перехвата трафика. Выявить наличие перехвата трафика непросто.	B	Потеря одного автомобиля. Злоумышленники будут целиться в данном случае на первую выигрышную регистрацию.	B
T4	Внесение в таблицу базы данных, используемых сайтом, запись с данными подставного лица.	B	Требуется средняя квалификация. Источник действия может быть и не вычислен (особенно в случае внешнего взлома)	B	Потеря автомобиля (ей).	B
T5	Взлом сайта. Например, для того, чтобы получить права администратора.	C	Требуется средняя квалификация. Вычисление злоумышленника, как правило, затруднительно.	B	Потеря автомобиля. В случае, если злоумышленнику удастся внести соответствующую запись в базе данных.	B
T6	Проведение DDoS-атаки	B	Требуется низкая квалификация. Финансовые затраты минимальны (200 USD за 24 часа атаки по данным из открытых источников).	C	На профильных сайтах может появиться негативная информация, что акция не проводится из-за атаки.	B
T7	Регистрация купонов в большом количестве.	B	Требуется низкая квалификация. Купоны легко собирать (например, сняв их с упаковок в магазинах)	B	Потеря автомобиля.	B

Еще раз обратим ваше внимание на то, что в случае существующей системы, зачастую необходимо в ходе оценки рисков учитывать наличие уязвимостей и эффективность внедренных контролей. Наверное, никто не будет спорить, что вероятность угона автомобиля возрастает в случае, если мы забываем ключи в системе зажигания. В тоже время оставленная фуражка сотрудника правоохранительных органов может

сработать, как «отпугивающий» (deterrent) контроль и снизить риск угона.

### Шаг 4. Ранжирование рисков

После проведенной оценки рисков мы сразу можем их ранжировать по значениям, и определять, какому риску уделить внимание в первую очередь, а какому - в последнюю. В нашем случае сначала будут высокие риски, связанные с угроза-

N	Угроза	Обработка риска	Остаточный риск
T1	Внесение логической закладки	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Разделение сред. Разработчики создают систему в своей «песочнице». В продуктивную среду коды приложений выкладываются администратором компании-организатора акции.</li> <li>Анализ исходного кода перед переносом в продуктивную среду.</li> </ul>	Н
T2	Ошибки программирования, ведущие к уязвимостям системы	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Анализ исходного кода перед переносом в продуктивную среду.</li> <li>Проверка защищенности системы перед вводом в эксплуатацию: сканирование, тестирование на проникновение.</li> </ul>	Н
T3	Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Использование шифрования трафика</li> <li>Выравнивание объемов передаваемых данных в ходе успешных и неуспешных регистраций.</li> </ul>	Н
T4	Внесение в таблицу базы данных, используемых сайтом, запись с данными подставного лица.	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Использование шифрования с открытым ключом для внесения данных участника акции. Закрытый ключ хранится у менеджера информационной безопасности до окончания акции.</li> </ul>	Н
T5	Взлом сайта. Например, для того, чтобы получить права администратора.	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Установка всех критичных обновлений безопасности</li> <li>Настройка системы в соответствии с принятыми в компании внутренними стандартами безопасности</li> <li>Проверка защищенности системы перед вводом в эксплуатацию: сканирование, тестирование на проникновение</li> </ul>	Н
T6	Проведение DDoS-атаки	<b>Передача:</b> <ul style="list-style-type: none"> <li>Сервер системы размещаем в датацентре провайдера. В соглашении с провайдером зафиксированы гарантии защиты ресурсов от DDoS-атак. Провайдер продемонстрировал нам, что соответствующие меры защиты от DDoS-атак внедрены и риск успешной атаки минимален.</li> </ul>	Н
T7	Регистрация купонов в большом количестве.	<b>Минимизация:</b> <ul style="list-style-type: none"> <li>Введение ограничения: 5 купонов на один IP-адрес с последующей блокировкой на 30 минут</li> </ul>	Н



ми T1-T5 и T7, а затем один средний риск - T6.

Это последний шаг нашей методики оценки рисков, но не последний во всем процессе управления рисками.

### *Обработка рисков*

После того, как мы оценили риски информационной безопасности, мы определяем варианты их обработки.

Выбор возможных действий с риском, к счастью, невелик: мы можем минимизировать риск, внедрив контрмеру(ы), передать его (страхование, аутсорсинг), избежать, изменив процесс или принять. Чаще всего мы минимизируем риски, а затем принимаем остаточные риски (residual risks).

В нашем случае, мы также решаем минимизировать большинство из них, внедрив соответствующие контроли и один передать внешнему дата-центру.

Необходимо отметить, что при внедрении системы менеджмента информационной безопасности, меры выбираются из каталога, приведенного в приложении А к стандарту ISO 27001.

### *Быстрые «победы» (quick wins)*

Зачастую, имеет смысл оценить необходимые для внедрения того или иного контроля ресурсы: финансовые, временные, людские. Наличие таких оценок позволит сделать две вещи: 1) выбрать наиболее экономически целесообразное решение проблемы 2) определить приоритеты по внедрению мер, так как имеет смысл в первую очередь минимизировать высокие риски с помощью недорогих мер (быстрые «победы»).

Остаточные риски должны быть осознанно приняты организацией (в лице владельца рисков).

### *Цикл PDCA и управление рисками*

Проведенная оценка рисков, выбор способов обработки рисков являются составляющей частью этапа «планирования» (Plan) цикла PDCA. Также на данном этапе формируется план внедрения мер с указанием сроков и ответственных лиц. На этапе «исполнения» (Do) данный план выполняется, на этапе «проверки» (Check) проверяется, что принятые меры работают, как следует, а на этапе «действия» (Act), выявленные недостатки исправляются.

### *Управление рисками и мотивация персонала*

Мы с вами понимаем, что наличие хорошо продуманных и формализованных процессов еще не является гарантией успешного функционирования системы менеджмента. Процессы работают тогда, когда работают люди, а люди работают, когда есть мотивация. В области управления рисками работающей практикой является ежегодная подготовка списков наиболее серьезных бизнес-рисков (например, ТОП 20 рисков компании). За

каждым риском, закрепляется владелец (обычно это человек «с полномочиями», топ-менеджер), который координирует деятельность по снижению данного риска в течение года. Если один риск повторно оказывается в следующем рейтинге ТОП 20, работа топ-менеджера по данной задаче признается неэффективной и он лишается части своей ежегодной премии.

### *Магическая формула ALE*

Для успешной сдачи экзамена CISSP необходимо помнить следующую формулу:

$$ALE = ARO * SLE,$$

где ALE (annualized loss expectancy) - ожидаемые потери в год, ARO (annual rate of occurrence) – частота возникновения инцидента течение года и SLE (single loss expectancy) – размер потерь в случае одного инцидента.

В определенных случаях данная формула может использоваться для количественной оценки рисков информационной безопасности.

Например, у нас есть с вами интернет-магазин. Рассмотрим риск его недоступности. Так как мы работаем на конкурентном рынке, в случае недоступности нашего веб-ресурса в течение дня наши клиенты несут свои деньги в магазины конкурентов, и мы теряем прибыль за день (пусть средняя ежедневная прибыль будет равна 100 000 рублей). У нас с вами есть статистика, что в среднем, наш магазин так «выключается» два раза год. Соответственно, можем вычислить ALE:

$$ALE = 2 * 100\,000 = 200\,000.$$

*Насколько научной должна быть методика оценки рисков?*

При проведении оценки рисков информационной безопасности необходимо помнить, что оценка рисков является составляющей процесса управления рисками, в который вовлечены специалисты различного уровня в нашей организации: от рядового сотрудника до генерального директора. Соответственно, применяемая методика должна быть понятна всем участникам процесса. В научной среде все поймут многоэтажные формулы, в среде коммерсантов - цифры потерь, а для большинства будет достаточно цветового обозначения в Excel: красный – высокий, желтый – средний, а зеленый – низкий риск.

### *Заключение*

В двух последних статьях мы рассмотрели систему менеджмента информационной безопасности и такую ее ключевую составляющую, как оценка и управление рисками ИБ [1, 2]. Понимание вопросов менеджмента информационной безопасности на уровне основных концепций облегчит сдачу

экзамена для получения статуса CISSP, так как экзамен все больше становится ориентированным на менеджеров ИБ. Для более глубокого погружения в вопросы управления ИБ рекомендуем читателям изучить стандарт ISO 27001:2013.

В следующей статье мы продолжим тему управления ИБ, но перейдем со стратегическо-

го уровня на операционный и рассмотрим темы домена «Операционная деятельность по обеспечению информационной безопасности» (security operations). Мы детально рассмотрим такие ключевые процессы информационной безопасности, как управление доступом, управление изменениями и другие [4-7].

### Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В. Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.
3. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности//Открытые системы. СУБД. 2007. № 8. С. 63-67.
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.
5. Michael E.Whitman, Herbert J.Mattord. Management of Information Security, Fourth Edition – Cengage Learning, 2014. 566 p.
6. Douglas J. Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.
7. Mark Sherling. Practical Risk Management for the CIO. – CRC Press, 2011. 385 p.

### References

1. Dorofeyev A.V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68.
2. Dorofeyev A.V., Markov A.S. Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii // Voprosy kiberbezopasnosti, 2014, No 1(2). pp. 67-73.
3. Markov A.S., Tsirlov V.L. Upravleniye riskami - normativnyy vakuum informatsionnoy bezopasnosti, Otkrytyye sistemy. SUBD, 2007, No 8, pp. 63-67.
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012, 968 p.
5. Michael E.Whitman, Herbert J.Mattord. Management of Information Security, Fourth Edition - Cengage Learning, 2014, 566 p.
6. Douglas J. Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.
7. Mark Sherling. Practical Risk Management for the CIO. – CRC Press, 2011. 385 p.

