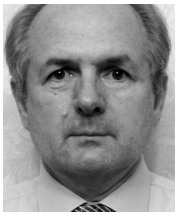
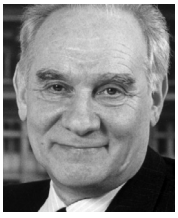
Новые возможности страхования информационных рисков: 15 лет спустя

Статья рекомендована Ю. Е. Хохловым 10.06.2015 г.

КОНЯВСКИЙ Валерий Аркадьевич
Доктор технических наук, профессор, научный руководитель ОАО «Конструкторское бюро полупроводникового машиностроения „Ростех“»



КУЗЬМИН Михаил Юрьевич
Начальник отдела ОАО «Конструкторское бюро полупроводникового машиностроения „Ростех“»



КРИСТАЛЬНЫЙ Борис Владимирович
Профессор, советник генерального директора ОАО «Конструкторское бюро полупроводникового машиностроения „Ростех“»

Аннотация
В статье рассмотрен ряд проблем, препятствующих, по мнению авторов, широкому распространению методов страхования информационных рисков в России. Выявлена наиболее значимая из них — проблема оценки безопасности информационных технологий, применяемых юридическими и физическими лицами, которая требует значительных затрат как со стороны страховых компаний (на проведение экспертизы информационных технологий), так и со стороны клиентов (на выполнение рекомендаций страховых компаний).
В статье предложены возможные методы снижения затрат на страхование информационных рисков, позволяющие расширить область страхования — от носителей информации и средств их обработки до информационных технологий и информационных систем в целом. Предложенный подход проиллюстрирован примерами применения новой инновационной отечественной импортозамещающей продукции — защищенных микрокомпьютеров на базе «гарвардских» микропроцессоров.
Практическая ценность рассмотренного в статье подхода заключается в том, что он может быть применен в страховании информационных рисков не только юридических, но и физических лиц. Это будет способствовать существенному расширению отечественного рынка доверенных информационных технологий с застрахованными информационными рисками.

Ключевые слова:
информационная технология, безопасность информационной технологии, информационная безопасность, информационный риск, страхование информационных рисков.

Страхование информационных рисков вот уже почти 15 лет является одной из самых трудно решаемых и в то же время актуальной проблемой в обеспечении информационной безопасности. С одной стороны, развитие и вместе с тем усложнение информационных технологий и применяемых в них средств и систем обусловливают *потребность общества* в непрерывном совершенствовании всех видов обеспечения информационной безопасности, включая методы страхования информационных рисков. С другой стороны, возрастает сложность и трудоемкость *оценки рисков* информационной безопасности информационных и других систем, используемых физическими и юридическими лицами (далее — клиентами).

В настоящей статье анализируются факторы, сдерживающие развитие страхования информационных рисков в России, формулируются предложения по решению этой актуальной задачи.

Понятие «информационная технология» рассматривается с точки зрения процессного подхода, согласно которому информационная технология есть совокупность регламентированных технологических процессов обработки (хранения, приема-передачи и др.) информации, включая ресурсы процесса — технические (аппаратные и программно-аппаратные) средства обработки информации и обрабатываемую информацию в виде данных на носителях информации, а также участвующий в реализации процесса персонал.

Нормативная база системы страхования информационных рисков в России

9 сентября 2015 г. исполнилось 15 лет с момента принятия старейшего правового документа в области информационной безопасности современной России — «Доктрины информационной безопасности Российской Федерации» [1]. До настоящего времени Доктрина является единственным основополагающим правовым документом, в котором в качестве экономического метода обеспечения информационной безопасности страны рассматривается «создание системы страхования информационных рисков физических и юридических лиц» (раздел 2, п. 5).

Для решения практических вопросов, связанных с созданием системы страхования информационных рисков, которая предусматривает компенсацию ущерба в случае реализации угрозы информационной безопасности, Указанием Госкомсвязи [2], действовавшим в период с 1998 по 2004 г., была создана специальная рабочая группа. Она включает представителей Госкомсвязи России, ведущих российских страховых компаний и организаций. Указание содержало Соглашение между участниками рабочей группы по сотрудничеству в области создания, развертывания и развития системы страхования информационных рисков, в том числе разработку правовых, нормативных и методических документов, финансирование проводимых работ, опытное внедрение страховых продуктов и осуществление страхования информационных ресурсов, систем и технологий. Ведущую роль в исследовательских работах в этой области выполнил Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации (ВНИИПВТИ). Среди страховых компаний первопроходцами и участниками рабочей группы стали «Промышленно-страховая компания», «Ингосстрах», «РОСНО», «Лидер», «Страховая акционерная компания „Информстрах“» и другие.

С целью развертывания системы страхования информационных рисков в России Указанием были рекомендованы разработанные базовые документы и/или их проекты:

- «Концепция страхования информационных рисков»;
- «Правила страхования (информационных рисков) информационных систем, информационных ресурсов, технических и программных средств вычислительной техники и оргтехники предприятий, организаций, учреждений и граждан»;

- «Методика управления информационными рисками»;
- «Методика оценки стоимости информационных систем, ресурсов, программных и технических средств вычислительной техники как объектов страхования»;
- «Положение и инструкция о проведении экспертизы информационных систем, технологий, программных ресурсов, технических и программных средств вычислительной техники при заключении договора страхования и при возникновении страхового случая», и другие.

В настоящее время использование страхования информационных рисков предусмотрено в ряде российских нормативных документов, в частности:

- «Концепция внедрения и использования информационных технологий» предусматривает страхование информационных рисков при создании «Интегрированной информационно-вычислительной системы Федерального агентства по рыболовству» [3];
- национальным стандартом по защите информации и обеспечению безопасности сетей электросвязи ГОСТ Р 52448 [4] установлено, что система обеспечения безопасности (СОБ) сетей электросвязи сети связи общего пользования является элементом системы информационной безопасности Российской Федерации; деятельность органов СОБ сети электросвязи, в частности, подразумевает «выполнение мероприятий по анализу информационных рисков, *созданию системы* управления рисками и *страхования информационных рисков*» (п. 8.4).

Методологическим и практическим вопросам применения в России системы страхования информационных рисков посвящены статьи [5—10] основоположников этой системы.

Типовые объекты страхования информационных рисков и оценка их страховых рисков

Как правило, каждая компания, осуществляющая страхование информационных рисков, использует собственную методику, определяющую объекты страхования и порядок оценки их рисков. В соответствии с существующей практикой, например, компании «Ингосстрах» [11], в качестве объектов страхования рассматриваются следующие активы:

- информационные активы: электронные данные (архивы, базы данных и др.) и программное обеспечение (компьютерные программы и системы);
- финансовые активы (денежные средства на счетах в банках);
- технические средства (компьютерное, телекоммуникационное и другое оборудование для хранения, обработки и передачи информации);

- профессиональная ответственность.

Страховыми рисками указанных объектов страхования, в частности, считаются:

- *для информационных активов* — утрата, уничтожение или повреждение застрахованных информационных активов вследствие: непреднамеренных ошибок в проектировании, разработке, создании, инсталляции, конфигурировании, обслуживании или эксплуатации информационных систем; совершенных компьютерных атак, действий компьютерных вирусов, а также умышленных противоправных действий клиента;
- *для финансовых активов* — утрата вследствие их неправомерного списания со счетов в результате ввода мошеннических команд в информационные системы, несанкционированной модификации программ, использование поддельного электронного платежного поручения, несанкционированного доступа к информационной системе клиента не уполномоченных на это лиц, а также умышленных противоправных действий клиента;
- *для технических средств* — их повреждение вследствие пожара, удара молнии, взрыва газа, стихийных бедствий, аварий инженерных коммуникаций, системы электроснабжения и т. п., а также кража, умышленное уничтожение или повреждение, ошибки в эксплуатации, изготовлении или монтаже;
- *для профессиональной ответственности* — непреднамеренная профессиональная ошибка при исполнении должностных обязанностей, непреднамеренное разглашение конфиденциальных сведений и коммерческой тайны, которые стали известны в связи с исполнением должностных обязанностей, в том числе и после увольнения.

Порядок оценки страховых рисков [10] предусматривает предоставление клиентом страховой компании сведений об объектах страхования, необходимых для получения общих сведений об объектах страхования, оценки их защищенности и т. п.

Компания, желающая застраховать информационные риски, перед заключением договора страхования должна пройти информационный аудит (аудит информационной безопасности), в рамках которого осуществляется оценка защищенности информационной системы (и/или информационной технологии) клиента. Информационный аудит, как правило, требует привлечения страховой компанией профессионального специалиста-аудитора в области информационных технологий и информационной безопасности. В результате обследования информационной системы и оценки ее защищенности аудитор формулирует рекомендации по устранению угроз информационной безопасности, регламентации процессов информационных технологий и др., при условии выполнения которых оплата страхового покрытия обойдется клиенту дешевле, поскольку выполнение рекомендаций уменьшает риски возникновения страхового случая. Например, для страхуемых информационных

активов (баз данных и программного обеспечения) должна быть предусмотрена возможность их восстановления, для финансовых активов и другой требуемой защиты (конфиденциальной, коммерческой и т. п.) информации должны применяться программно-технические средства их защиты.

Если в течение срока действия полиса у клиента произошли изменения используемой информационной технологии, которые могут повлечь изменение степени риска, то в соответствии с Информационным сообщением Совбеза РФ [12] (ст. 959) клиент обязан уведомить об этом страховую компанию. Страховая компания имеет право назначить процедуру повторного информационного аудита, результат которого может повлечь изменение условий страхования и увеличение суммы страховой премии в случае возрастания рисков объектов страхования.

Факторы, сдерживающие распространение страхования информационных рисков

Исходя из описания процесса оценки информационных рисков объектов страхования, можно определить, что же ограничивает массовое применение страхования информационных рисков.

Во-первых, это достаточно затратный для клиента информационный аудит, который сопоставим по выполняемым работам и необходимым ресурсам с аудитом информационной безопасности или с аттестацией информационных систем[1]. Небольшие организации могут не располагать необходимыми финансовыми средствами.

Во-вторых, информационный аудит требует наличия у клиента полностью регламентированной информационной технологии, без которой невозможно оценить защищенность объектов страхования и, следовательно, связанные с ними информационные риски. Не секрет, что подобная регламентация является неосуществимой мечтой для подавляющего числа организаций-клиентов.

В-третьих, даже в небольших компаниях применяемая информационная технология достаточно часто претерпевает изменения, вызванные, в частности, необходимостью использования нового прикладного программного обеспечения, модернизацией технических средств и т. п. Об этих изменениях клиент должен сообщить страховой компании, которая принимает решение о повторном проведении информационного аудита, что предполагает дополнительные затраты клиента на страхование.

Все сказанное относится к клиентам, являющимся юридическими лицами. Что касается физических лиц, то в открытом доступе в сети интернет, включая сайты российских страховых компаний, отсутствуют сведения

[1] Одной из проблем, требующих решения при информационном аудите, является трудность локализованного (изолированного) рассмотрения объекта страхования, т.е. выявления и учета зависимости объекта страхования от других компонентов информационных систем, которые могут оказывать влияние на безопасность рассматриваемого объекта.

о фактах проведения в России аудита информационных технологий и систем, принадлежащих физическим лицам, а также о страховании ими информационных рисков. Возможно, дело здесь в том, что информационные технологии используются физическими лицами в личных целях и что для некритичных информационных технологий затраты на ликвидацию последствий их нарушений в случае реализации угроз информационной безопасности могут оцениваться людьми как значительно меньшие по сравнению с затратами на информационный аудит и страхование информационных рисков. Для критичных информационных технологий, например, использования систем электронных платежей, затраты на страхование информационных рисков могут представлять серьезную финансовую проблему для многих физических лиц в основном из-за необходимых затрат на выполнение требований информационного аудита.

Можно сделать вывод, что расширению российского рынка страхования информационных рисков способствовало бы *снижение затрат* клиентов на первичный и повторный информационный аудит и на страхование информационных рисков в целом. В этом случае страхование информационных рисков будет доступно по стоимости не только юридическим, но и физическим лицам.

Существенное снижение затрат на аудит может быть достигнуто путем:

- применения клиентами специфицированных, регламентированных и защищенных информационных технологий, средств и систем;
- наличия гарантированной неизменности информационной технологии, реализуемой программно-аппаратными средствами;
- максимального снижения вероятности непреднамеренного или умышленного изменения информационной технологии пользователями информационной системы.

Указанные требования к информационным технологиям могут быть реализованы с помощью некоторых современных средств обработки информации.

Как обеспечить регламентированность, защищенность и гарантированную неизменяемость информационной технологии

В качестве примера, иллюстрирующего применение предложенного подхода к страхованию информационных рисков, рассмотрено использование физическими и юридическими лицами инновационной отечественной импортозамещающей продукции — защищенных микрокомпьютеров на базе «гарвардских» микропроцессоров, производимых ПАО «Трастед Клауд Компьютерс-миллионер».

К числу особенностей защищенных микрокомпьютеров на базе «гарвардских» микропроцессоров относятся:

- принципиальная невозможность осуществить запись в память, занимаемую программой, исключает вероятность разрушения программ в случае их сбоев при обработке данных или компьютерных атак;
  Примечание. В процессорах традиционной «фон-неймановской» архитектуры (основа большинства используемых персональных компьютеров) такого свойства нет, поэтому в системах на их базе требуются дополнительные средства защиты.
- динамически изменяемая архитектура, которая обеспечивает необходимую защищенность и эффективность;
- обеспечение неизменности операционной системы и прикладных программ;
- обеспечение «вирусного иммунитета»;
- возможность адаптации «стандартных» операционных систем для микрокомпьютеров.

Используемая в микрокомпьютерах новая архитектура позволяет:

- существенно повысить защищенность клиентских компьютеров;
- значительно снизить стоимость защиты;
- обеспечить создание защищенного облака (one touch security);
- создать защищенные клиентские компьютеры (локальные, сетевые, облачные), планшеты, телефоны и др.

Состав линейки защищенных микрокомпьютеров:
1) микрокомпьютеры МКТ и МКТ+ (рис. 1) представляют собой

- микрокомпьютеры в форм-факторе донгла (большой флешки), работающие только в защищенном режиме;

Рис. 1 Микрокомпьютеры МКТ и МКТ+

- отличие МКТ+ от МКТ — возможность обновления защищенной операционной системы (ОС) в специальном технологическом режиме (в сервисном центре);
- перевод в технологический режим осуществляется физическим, а не программным воздействием, что обеспечивает невозможность несанкционированной программной модификации;
- переключатель режимов находится внутри корпуса устройства и недоступен пользователю.

Технические характеристики:

- операционная система: защищенная ОС Linux;
- встроенная память: 8GB с доступом «только чтение»;
- поддержка микрокарт памяти до 32 ГБ;
- сеть: WiFi 802.11b/g/n; Bluetooth 2.1;
- интерфейс HDMI;
- поддержка 1920x1080P @60 Гц, HD-видео;
- порты: Micro USB 2.0 DC, 1 x Micro USB OTG1 x USB 2.0, слот для Карт TF, порт HDMI;
- подключается:
к телевизору или проектору через порт HDMI;
к монитору — через DVI;
- питание: от USB-порта телевизора или монитора, или внешнего блока питания (5V-2A).

2) Микрокомпьютер МКTrusT (рис. 2) представляет собой

Рис. 2 Микрокомпьютер МКTrusT

- микрокомпьютер в форм-факторе донгла (большой флешки), работающий в одном из двух режимов на выбор — защищенном или обычном (без ограничений);
- выбор режима осуществляет пользователь физическим переключателем;
- в каждом режиме используется своя ОС — защищенная или обычная;
- ОС физически и технологически разделены между собой во время хранения и работы;
- незащищенная ОС обновляется как любой Android, защищенная — как в МКТ+.

Технические характеристики:

- операционная система: защищенная — Linux собственной сборки; незащищенная — Android;
- подключается: к телевизору или проектору через порт HDMI; к монитору — через DVI;
- питание: от USB-порта телевизора или монитора, либо внешнего блока питания (5V-2A);
- подключение к интернету осуществляется по WiFi.

3) Терминальная станция МКТ-card (рис. 3) представляет собой

- терминал, состоящий из стационарной док-станции, к которой подключается периферия, и отчуждаемого мобильного устройства — носителя всей персонифицированной части информационной среды клиентского рабочего места;
- МКТ-card и МКТ-card long — это доверенный облачный микрокомпьютер с динамически изменяемой архитектурой.

Технические характеристики:

Рис. 3 Терминальная станция МКТ-card

- параметры компьютера аналогичны остальным решениям линейки;
- док-станция содержит: 8 USB-портов; выход HDMI; сетевой разъем RJ-45; разъем питания;
- док-станция коммутируется: с периферийным оборудованием через USB; с монитором через HDMI; с сетью — через RJ-45; возможно использование WiFi (при условии разрешения на его применение).

4) Планшетный компьютер TrusTPad (рис. 4) представляет собой

- планшетный компьютер, построенный на «гарвардской» архитектуре по логике MKTrusT;
- имеет аналогичные MKTrusT возможности: работы в одном из двух режимов — защищенном или обычном; выбора защищенного или обычного режима с помощью переключателя; обновления защищенной и обычной ОС.

Технические характеристики: параметры TrustPad аналогичны параметрам MKTrust, за исключением наличия у планшета экрана.

Особенности микрокомпьютеров:

- в них используется принципиально новая архитектура на базе «гарвардских» процессоров;
- чтобы начать работать достаточно подключить микрокомпьютер к телевизору или монитору;
- для работы в защищенном и обычном режимах применяются две независимые ОС;
- неизменность защищенной ОС обеспечивается аппаратным способом;
- в них используется доверенная программная среда;
- вычислительные характеристики аналогичны офисным ПК;

Рис. 4 Планшетный компьютер TrusTPad

- осуществляется поддержка идентификации и аутентификации клиента при защищенном соединении;
- соблюдение принципа «моя информационная среда всегда со мной»;
- имеются встроенные сертифицированные средства электронной подписи и шифрования;
- осуществляется поддержка работы с защищенными ключевыми носителями по протоколу CCID;
- осуществляется поддержка управления проводными (USB) и беспроводными (2.4 Ghz, bluetooth) мышками, клавиатурами и пультами;
- используется физический переключатель выбора защищенного или обычного режима работы;
- технологически невозможно программное воздействие на выбор режима работы;
- рабочее место на базе планшета может использоваться не только как клиентская часть централизованной инфраструктуры, но и как автономное рабочее место;
- при необходимости использования каких-либо источников или хранилищ данных при работе в защищенном режиме в качестве защищенного локального хранилища могут использоваться служебные носители, например, семейства «Секрет»;
- простота использования, не требующая от пользователей специальных знаний в области защиты информации;
- решения по защитным механизмам в доверенных средах микрокомпьютеров основаны на 12 российских патентах разработчика.

Возможности микрокомпьютеров:

- защищенный доступ и работа с корпоративными приложениями и сервисами в традиционных и облачных инфраструктурах;
- доступ к интернет-сервисам, приложениям из Google Play Store и т. п. и их использование;
- работа с офисными документами, электронными изданиями, книгами, медиа-контентом и др.;
- подписание и проверка электронной подписи, криптозащита электронных документов;
- совершение покупок и оплата различных услуг через интернет;
- безопасная в защищенном режиме работа с критичными к защищенности сервисами;
- работа в незащищенном режиме — без ограничений возможностей со стороны изделий;

- обновления ОС в доверенной среде.

Области применения:

- доступ к защищенным информационным системам, в том числе в корпоративных сетях;
- доступ к госуслугам и их получение в электронном виде;
- проведение видеоконференций в различных вариантах — телемедицинские консультации, дистанционное образование и др.;
- участие в интернет-торговле с обеспечением должного уровня информационной безопасности;
- безопасное управление банковским счетом, включая электронные платежи;
- обработка персональных данных;
- использование электронной подписи и шифрования при работе с официальными документами в электронном виде;
- доступ к аудио- и видео- on-line контенту с современным уровнем качества (потоковое видео и видеофайлы с качеством FullHD);
- доступ к интернету, электронной почте, видеотелефонии (Skype и др.), социальным сетям, сервисам интернет-кинотеатров (iviRU, MegogoNET и др.), компьютерным играм и др.;
- доступ ко всем другим «благам цивилизации», когда необходимо использование универсального мобильного устройства с возможностью его применения в режимах, требующих повышенной защищенности, и в обычном режиме.

При применении микрокомпьютеров в защищенном режиме обеспечивается конкретная регламентированная и описанная в документации информационная технология, которая гарантированно неизменяема, т.к. в процессе работы у пользователя просто нет средств для непреднамеренного или умышленного ее изменения. В частности, пользователь может использовать такой микрокомпьютер для защищенной работы в системе «клиент–банк» для совершения электронных платежей, будучи уверен в том, что со стороны клиента системы гарантированно обеспечивается выполнение регламентированной технологии взаимодействия с банком.

Указанные свойства и характеристики микрокомпьютеров позволяют не проводить информационный аудит каждого микрокомпьютера, применяемого юридическим или физическим лицом в определенной информационной технологии, что существенно снижает расходы клиентов на оценку страхуемых ими информационных рисков.

Гарантированная микрокомпьютером защищенность и неизменность используемой информационной технологии позволяет страховой компании легко оценить страхуемые информационные риски клиента как

практически нулевые (ненулевой вклад в риски дает, например, возможная поломка или потеря микрокомпьютера. В последнем случае использовать микрокомпьютер посторонний пользователь не сможет). Величина страховой премии клиента при использовании таких микрокомпьютеров будет весьма незначительной.

Таким образом, за счет применения средств, аналогичных рассмотренным микрокомпьютерам, которые обеспечивают регламентированность, защищенность и гарантированную неизменяемость используемой информационной технологии, российский рынок страхования информационных рисков, по нашему мнению, может быть расширен, в том числе за счет охвата страхованием физических лиц.

* * *

Современный уровень развития информационных технологий открывает новые возможности для развития системы страхования информационных рисков в России. В первую очередь это связано с применением доверенных элементов информационных технологий — средств обработки информации, обеспечивающих и гарантирующих защищенность и неизменность реализуемой с их помощью информационной технологии. Гарантированная защищенность и неизменность информационных технологий существенно снижает риски их применения, что дает возможность страховым компаниям, с одной стороны, снизить размер страховой премии, а с другой — повысить страховые выплаты.

Во-вторых, использование доверенных информационных технологий существенно снижает затраты на оценку их безопасности страховыми компаниями и затраты клиентов на выполнение рекомендаций по снижению рисков безопасности применяемых ими информационных технологий. Гарантированная защищенность и неизменность информационной технологии исключает необходимость затрат на ее переоценку страховыми компаниями.

В-третьих, применение доверенных, защищенных от изменения информационных технологий открывает широкие возможности для страхования информационных рисков физическими лицами, которые в настоящее время практически не охвачены этой системой, например, для страхования рисков нарушения целостности информационной системы «клиент–банк» и в целом безопасности финансовых операций с ее использованием.

В-четвертых, предложенный подход позволяет осуществлять поставку доверенных информационных технологий в виде комплексного пакета, содержащего, например, доверенное средство информационных технологий и типовой полис страхования информационных рисков применения этого средства физическим лицом для осуществления электронных платежей.

Использование доверенных информационных средств и систем с гарантированно неизменяемой реализуемой ими информационной технологией является основой для дальнейшего развития систем страхования информационных рисков в России. В апреле 2015 г. Совет безопасности РФ сообщил о начале разработки новой редакции Доктрины информационной

безопасности Российской Федерации [13]. Среди четырех основных составляющих национальных интересов страны в информационной сфере (п. 1 раздела 1) предусмотрена «защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем».

Учитывая существующую в России практику применения страхования информационных рисков и новые возможности, позволяющие использовать гарантированно неизменные и защищенные информационные технологии, можно полагать, что страхование информационных рисков останется в новой редакции Доктрины в перечне методов обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. **Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 09.09.2000 № Пр-1895.**

2. **Указание Госкомсвязи РФ от 04.12.1998 № 121-у «О реализации Соглашения о сотрудничестве в области страхования информационных рисков» (вместе с Соглашением от 10.11.1998 № 6836).**

3. **Приказ Росрыболовства от 12.10.2009 № 896 «Об утверждении Концепции внедрения и использования информационных технологий в деятельности Росрыболовства, его территориальных органов и находящихся в его ведении организаций».**

4. **ГОСТ Р 52448—2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.**

5. КОНЯВСКИЙ В. А., ХОВАНОВ В. Н. **Роль и место системы страхования информационных рисков в обеспечении информационной безопасности** // Управление защитой информации. 2009. С. 15—22. http://www.pvti.ru/data/file/part3.pdf

5. КОНЯВСКИЙ В. А., ХОВАНОВ В. Н. **Страхование информационных рисков и обеспечение информационной безопасности** // Управление защитой информации. 2000. № 1. http://www.okbsapr.ru/index_hovanov.html

6. КОНЯВСКАЯ С. В. **Страхование информационных рисков: подводные камни** // Information Security. 2007. № 6—1 (декабрь 2006 — январь 2007). С. 58, 59.

7. КОНЯВСКИЙ В. А., ХОВАНОВ В. Н. **Система страхования информационных рисков как экономический механизм компенсации ущерба при воздействии угроз информационной безопасности** // ИНФОРМОСТ — Средства связи. 2003. № 15.

8. КОНЯВСКИЙ В. А. **Мобильные платежи — проблемы и пути решения** // Комплексная защита информации. Материалы XI Международной конференции. 20—23 марта 2007 г. Новополоцк. 2007. С. 135. http://www.okbsapr.ru/konyavski_2007_2.html

9. МАКАРЕНЦЕВ А. **Страховой backup** / Консультант. 2009. № 13.

10. **Компания «Ингосстрах». Страхование рисков в области информационных технологий и телекоммуникаций.** http://www.ingos.ru/ru/corporate/communications/

11. **Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 06.04.2015, с изменениями от 07.04.2015).**

12. **Информационное сообщение Совета Безопасности Российской Федерации от 07.04.2015 о начале разработки новой редакции Доктрины информационной безопасности Российской Федерации.** http://www.scrf.gov.ru/news/874.html