DOI 10.22394/1726-1139-2018-7-174-182

Локализация коммуникаций как способ обеспечения информационной безопасности

Павлов В. В.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; pavlov1101leti@mail.ru

РЕФЕРАТ

В статье анализируется технологический аспект информационной безопасности. Отмечается уязвимость использования в качестве основного инструмента передачи данных глобальной сети интернет. В качестве альтернативы рассматривается идея использования локальных сетей передачи данных как инструмента информационной безопасности. Использование локальных коммуникационных сетей для передачи конфиденциальной информации снижает возможность несанкционированного доступа. Были рассмотрены принципы построения беспроводных сетей передачи данных, их недостатки и способы модернизации для обеспечения быстрой и надежной передачи данных.

Ключевые слова: информационная безопасность, локальная сеть, беспроводная связь, маршрутизация

Localisation of Communication Lines as the Way of Providing the Safety of Information

Pavlov V. V.

Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management of RANEPA), Saint-Petersburg, Russian Federation; pavlov1101leti@mail.ru

ABSTRACT

The article is focused specially on the technological aspect of the safety of information. Insecurity of using the global network Internet as a main instrument for data transmission is also pointed. The idea of using the local network data transmission is taken into account as an alternative. The usage of locals networks for the transmission of non-public information excepts the possibility of an unauthorized access. The principles of construction of the data transmit local networks, its problems and the ways of its modernization for providing the fast and resilient transmission have been analyzed as well.

Keywords: The safety of information, local network, wireless communication, routing

Введение

Проблема информационной безопасности имеет, по меньшей мере, два аспекта, которые могут быть сведены, если использовать выражение российских исследователей Т. В. Владимировой и В. Н. Илюшенко, к «защите информации и защите от информации» [2, с. 24; 5, с. 3]. Первый аспект — преимущественно технико-технологический, где речь идет о защите конфиденциальной (скрытой) информации от несанкционированного проникновения, а также информационной инфраструктуры от деструктивного внешнего воздействия. В настоящее время в нашей стране появилось немало исследований, касающихся технологической стороны информационной безопасности, но они посвящены, главным образом, вопросам защиты информации в компьютерных системах и сетях [3, 4, 17], немало внимания уделяется и такой стороне информационной защиты, как криптография [13].

Второй аспект — социокультурный, который предполагает защиту мировоззренческих основ общества, его культуры, обычаев и традиций от чрезмерного внешнего, инокультурного влияния. Ему посвящена обширная литература, касающаяся самых разных сторон жизни общества. В частности, большое внимание информационному противоборству в мировой политике и международных отношениях уделяется в работах Ю. В. Косова [10], информационные угрозы и информационная безопасность государства в контексте международных отношений получили свою разработку в целом ряде работ В. П. Кириленко и Г. В. Алексеева [6, 7, 8]; коммуникативные аспекты военной безопасности нашли развитие в исследованиях А. А. Ковалева и Е. И. Кудайкина [9]; в исследованиях А. В. Морозова и Т. А. Поляковой [14, 15] получили отражение вопросы «организационного и правового обеспечения информационной безопасности и электронного взаимодействия в рамках единого информационного пространства Российской Федерации» [14, с. 10], правовой стороне функционирования интернета посвящена работа И. М. Рассолова [16] и т. д.

В настоящей работе мы сосредоточимся на первом аспекте, и в центре нашего внимания будут вопросы локализации систем информационного обмена как одного из способов обеспечения информационной безопасности.

Цель настоящей работы состоит в том, чтобы показать, с одной стороны, уязвимость использования в качестве главного инструмента информационного обмена глобальной сети интернет и — с другой — обосновать возможности, которые предоставляют локальные сети и одновременно выявить связанные с ними ограничения.

Материалы и методы

В предлагаемом исследовании автор использовал метод сравнения, с помощью которого выявлял достоинства и недостатки, а также ограничения в работе открытых и закрытых (локальных) информационных сетей. В работе показано, что самая совершенная на сегодняшний день система передачи информации — глобальная сеть интернет — не отвечает критерию безопасности передаваемой информации. Кроме того, ее применение ставит пользователя под контроль так называемой «нетократии» — «владельцев сети» или новой правящей элиты, по меткому выражению шведских исследователей А. Барда и Я. Зодерквиста [1, с. 5].

В качестве альтернативы, обеспечивающей безопасность информационного обмена, могут быть предложены локальные сети. Для их анализа автор использовал методологию теории графов, в частности, применяемые в теории графов алгоритмы поиска кратчайшего пути для обеспечения эффективности и надежности коммуникации («алгоритм Дейкстры») [20, p. 269–271]. Данная методология предполагает использование серьезного математического аппарата, однако автор решил воспользоваться рекомендацией С. Хокинга, который советовал не злоупотреблять формулами, дабы не усложнять чрезмерно текст [19, с. 5] и предпочел нематематический способ изложения материала. И все-таки одну — известную «формулу Шеннона» — для проверки выдвинутой гипотезы пришлось использовать. Авторская гипотеза состоит в том, что принятый в качестве кратчайшего (в смысле удаленности) маршрут передачи информации не всегда является оптимальным с точки зрения надежности и эффективности.

Результаты

Оптимальность работы локальной информационной сети в настоящей работе определяется не столько выбором кратчайшего расстояния между источником и адресатом информационного сообщения, сколько выбором такого маршрута, который

обеспечивает минимум потерь и искажений передаваемой информации и высокую пропускную способность канала.

Обсуждение

Развитие современных систем передачи информации значительно повлияло на коммуникацию в мире с точки зрения объема и скорости передаваемой информации. Еще в 60-е годы XX столетия известный канадский ученый — филолог, литературовед, исследователь массмедиа — М. Маклюэн отмечал, что открытие электромагнитных волн «вновь создало симультанное «поле» всех человеческих действий, благодаря чему человеческий род теперь существует в условиях «глобальной деревни» [11, с. 47], где «каждому в мире приходится теперь жить в условиях предельной близости с другими, созданной нашим электрическим вовлечением в жизнь друг друга» [12, с. 44], а человеческая жизнь «как частная, так и социальная — была выведена в поле всеобщего обозрения» [12, с. 57]. Сегодня требования к скоростям становятся все выше, а системы беспроводной связи все больше расширяют свою функциональность.

Современные стандарты передачи представляют собой системы мобильной связи четвертого поколения 4G (fourth generation). Технология 4G имеет заявленную скорость беспроводной передачи данных — 100 Мбит/с. На практике, однако, эта скорость ограничена единицами или десятками Мегабит. Тем не менее, даже такой скорости вполне достаточно для комфортного, сравнимого с проводной, пользования сетью, доступа в интернет и обмена данными. Развитие подобных технологий активно продолжается, не за горами появление новых поколений беспроводных стандартов, из чего можно сделать предположение, что данная тенденция сохранится и далее.

На фоне столь бурного процветания стандартов беспроводного соединения возникает вопрос о целесообразности построения локальных систем передачи данных. Может возникнуть вопрос: а зачем разворачивать локальную сеть, когда быструю и надежную передачу информации легко осуществить через интернет? Действительно, глобальная сеть интернет представляется идеальной коммуникационной системой с точки зрения скорости и объема передаваемых с ее помощью данных. С другой стороны, она не отвечает требованиям безопасности и защиты передаваемой информации. По аналогии с обыкновенной деревней, где «все про всех все знают», в «глобальной деревне», создаваемой всемирной паутиной, в общем доступе тоже может оказаться слишком много информации, не предназначенной для других. Это во-первых. Во-вторых, всегда следует помнить о том, кто и с какой целью создавал глобальную сеть, и в чьих руках находятся рычаги контроля над ней.

Сегодня, в условиях обострения международной обстановки и политики санкций со стороны западных стран, всерьез обсуждается гипотетическая возможность отключения России от сети интернет. Об этом, в частности, в начале марта 2018 г. в эфире телеканала НТВ говорил директор и владелец интернет-компании LiveInternet, советник Президента РФ Г. Клименко[1]. Он подчеркнул, что ситуация вполне вероятная, поскольку уже есть примеры отключения Крыма от сервисов Google и Microsoft. За этим могут последовать новые шаги, и мы должны быть к ним готовы.

Следует отметить, что такого рода опасность осознавалась и ранее. Еще в 2010 г. было принято распоряжение Правительства РФ № 2299-р, утверждающее план перехода федеральных органов исполнительной власти и федеральных бюджетных

[1] Эксклюзивное интервью советника Президента РФ по интернету Германа Клименко. Полная версия [Электронный ресурс]. URL: https://www.youtube.com/watch?v=FzEigDn4d-U (дата обращения: 11.03.2018).

учреждений на использование свободного программного обеспечения на 2011–2015 гг.[1] Речь шла о разработке и внедрении пакета отечественного программного обеспечения, включающего операционные системы, драйверы для оборудования и прикладное программное обеспечение для серверов и рабочих мест пользователей. В 2014 г. в Минсвязи начал разрабатываться план мероприятий на случай, если западные страны, в первую очередь США, попытаются заблокировать для России доступ к интернету, воспользовавшись тем, что большая часть компонентов сетевой инфраструктуры находится не на территории России и управляется извне.

Следующим шагом стал подписанный Президентом РФ В. В. Путиным Указ № 260 «О некоторых вопросах информационной безопасности Российской Федерации», который предполагал преобразование сегмента международной компьютерной сети интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящегося в ведении Федеральной службы охраны РФ, в российский государственный сегмент информационно-телекоммуникационной сети интернет, являющийся элементом российской части сети интернет. Государственный сегмент сети интернет предназначался, во-первых, для подключения к нему государственных информационных систем и информационно-телекоммуникационных сетей государственных органов и тех организаций, которые создавались для выполнения задач, поставленных для федеральных государственных органов; во-вторых, для размещения в сети интернет информации государственных органов и указанных выше организаций.

Указом устанавливалось, что до 31 декабря 2017 г. к государственному сегменту сети должны подключиться Администрация Президента РФ, Аппарат Правительства РФ, Следственный комитет РФ, федеральные органы исполнительной власти и органы исполнительной власти субъектов РФ. То же самое рекомендовано сделать обеим палатам Федерального собрания РФ, органам прокуратуры, Счетной палате, а также организациям, созданным для выполнения задач, поставленных перед федеральными государственными органами. При этом подключение к государственному сегменту сети должно осуществляться по каналам передачи данных, защищенных с использованием шифровальных (криптографических) средств (защищенным каналам).

Сегодня можно констатировать, что мы располагаем техническими возможностями для перехода на российский сегмент сети интернет. Это отмечал в упомянутом выше интервью Г. Клименко, при этом он подчеркивал, что, с точки зрения программно-аппаратной, серьезных сбоев при таком переходе быть не должно — наша зависимость в плане программного обеспечения не так велика, как кажется. Больше всех могут пострадать те, кто хранит данные за рубежом. Вместе с тем, следует отметить, что идти по китайскому пути намеренной самоизоляции Россия не собирается: речь идет не об отключении страны от интернета, а о плане мероприятий на тот случай, если Запад попытается заблокировать для России доступ к сети.

Таким образом, локализация глобальной сети может стать, во-первых, следствием политики противоборства на международной арене и санкций (теперь уже информационных); во-вторых, естественной реакцией на эту политику с целью защиты своих интересов в информационной сфере и обеспечения информационной безопасности.

Требованиям безопасности больше отвечает создание многочисленных локальных сетей с закрытым доступом к глобальной сети. Передавая по локальной сети

[1] Правительство Российской Федерации. Распоряжение от 17 декабря 2010 г. № 2299-р [Электронный ресурс]. URL: http://minsvyaz.ru/common/upload/2299p.pdf (дата обращения: 12.03.2018).

конфиденциальную информацию, доступ к которой разрешен только пользователям данной сети, мы снижаем возможность взлома, хакерских атак, несанкционированного доступа, утечки информации или намеренного ее искажения, которые хорошо известны пользователям интернета. Польза от применения подобных сетей очевидна во всех случаях, когда по тем или иным причинам информация, передаваемая между участниками сети, конфиденциальна, а обмен ею должен быть защищен.

Именно поэтому локальные сети передачи данных активно используются военными, различными ведомствами, крупными корпорациями для передачи служебной информации, применяются они также в охранных системах, системах видеонаблюдения, управлении техническими процессами на предприятиях и во многих других случаях.

В силу огромных размеров страны, значительных расстояний между объектами и труднодоступности многих территорий и объектов придется, по-видимому, создавать локальные сети на основе радиоканалов. Локальные сети передачи данных на основе радиоканалов базируются на совокупности двух групп технологий — беспроводной передачи информации и сетевого взаимодействия. Безусловно, любой радиоканал является уязвимым объектом, поэтому для защиты передаваемой информации от радиоперехвата используется, в простейшем случае, дополнительное кодирование сигнала, тогда даже в случае его обнаружения в эфире другими станциями, быстро извлечь из него информацию, не зная ключей, не удастся.

В данной работе мы не будем подробно рассматривать методы кодирования, приняв их высокий уровень защиты информации «по умолчанию». Но даже в том случае, когда передаваемая информация, в общем, не является секретной, ее точность, достоверность и своевременность могут быть социально значимыми, если речь идет, к примеру, о мониторинге и контроле энергосетей, газоснабжения, о системах предупреждения чрезвычайных ситуаций природного или техногенного характера и т. д. Именно поэтому нас здесь больше интересуют вопросы, связанные с проблемой своевременной, надежной и устойчивой передачи информации по локальным сетям, решение которой также является неотъемлемой частью информационной безопасности, как и национальной безопасности в целом. Своевременность, точность и полнота информации — необходимая основа принятия правильных и адекватных сложившейся ситуации решений. Точность и полнота информации не обязательно гарантируют правильность решения, но они создают потенциальную возможность для его принятия.

Разумеется, различные локальные сети имеют конструктивные отличия в зависимости от назначения, требований к защите, стоимости и сложности аппаратуры, типа передаваемых данных, требований к каналам и т. д. Однако существуют общие проблемы функционирования сетей самого разного типа, связанные с маршрутизацией. Именно на эти проблемы мы хотели бы обратить внимание.

В случае, когда связывающиеся пункты (участники сети) расположены дальше достижимой дальности радиосвязи, информационная связь с такими пунктами обеспечивается посредством ретрансляции сигналов промежуточными пунктами. То есть пункты (один или несколько), расположенные территориально между двумя удаленными, общающимися пунктами, играют роль ретрансляторов. Несмотря на то, что ретрансляция сообщений позволяет существенно расширить территорию, охватываемую сетью, здесь может возникнуть ряд трудностей, которые предстоит разрешить.

Речь идет о том, что большинство сетевых комплексов при организации маршрутов применяет фиксированную маршрутизацию. Это означает, что маршрут (т. е. совокупность пунктов-ретрансляторов), по которому проходят сообщения, отправляемые друг другу двумя «невидимыми» напрямую пунктами, назначается один раз и без возможности его изменения. Как правило, такой фиксированный маршрут передачи

сообщений является оптимальным, поскольку ретрансляторы, при нескольких возможных, безальтернативно назначаются из соображения кратчайшего расстояния между ними. Составление маршрутной карты из соображений кратчайшего пути невозможно для подвижных объектов (что естественно, ибо изменение местоположения приводит и к изменению расстояния), и может применяться только для тех объектов, расположение которых неизменно — т. е. для стационарных объектов.

Однако тут имеется серьезный недостаток, ибо мы живем не в «свободном» пространстве с постоянными и неизменными характеристиками, где ослабление энергии сигнала зависит только от расстояния, а в реальной среде, где факторами, влияющими на прием сигналов, являются шумы, помехи от внешних электронных устройств, сложный рельеф местности, специфика распространения радиоволн и т. д. Из этого следует вывод, что наименьшее расстояние еще не является гарантией лучшей и более надежной связи.

Сама же фиксированная маршрутизация также не является надежной, поскольку выход из строя одного из промежуточных пунктов, или ухудшение условий передачи сигналов на определенном участке, где расположен этот пункт, приведет к потере связи с ним самим, а также с теми пунктами, для которых он является ретранслятором. Поэтому важным этапом модернизации сетей является альтернативная маршрутизация, которая предполагает возможность использования, помимо основного маршрута передачи, некоторое количество альтернативных маршрутов, а также возможность самой сети выбирать маршрут передачи путем проверки состояния трассы, по которой распространяется сигнал.

Не требует доказательств положение, что при фиксированных параметрах технических средств именно расстояние является ключевым фактором ослабления сигнала. Однако в реальных условиях любой физический процесс всегда подвержен внешним воздействиям, контролировать которые мы зачастую не в состоянии. В результате можно сделать вывод, что наименьшее расстояние совсем не обязательно является непреложным условием эффективности работы канала.

Существуют и другие параметры (метрики), по которым происходит оценка канала — задержка, пропускная способность, вероятность ошибки. Метрики могут быть как одинарные, так и комбинированные. Задержка может сильно колебаться в зависимости от температуры в трактах передающей и принимающей аппаратуры, т. е. является непостоянным параметром. Пропускной способностью называется верхняя граница скорости передачи данных, с которой может быть задана низкая вероятность ошибки.

Пропускная способность канала связи рассчитывается по формуле Шеннона:

$$C = W \cdot \log\left(1 + \frac{P}{N}\right)$$

где C — пропускная способность, W — полоса пропускания канала, P — мощность полезного сигнала, N — мощность шума [18, с. 310].

Хотя реальная скорость передачи сигналов всегда ниже, пропускная способность является одной из наиболее важных характеристик канала связи. Именно она, в первую очередь, принимается во внимание при выборе канала, по которому будет осуществляться передача информации. Пропускную способность можно вычислить между двумя пунктами (участниками сети), однако, если маршрут пролегает через промежуточные пункты (ретрансляторы), то определение общей пропускной способности для всего маршрута крайне затруднительно, если вообще возможно. Согласно приведенной выше формуле Шеннона, пропускная способность зависит от полосы пропускания канала W, которая по умолчанию фиксирована, и отношения сигнал/шум (P/N). Но все дело в том, что природа шумов различна,

и в каждом конкретном случае их комбинация может быть уникальной, хотя наибольший вклад вносит тепловой шум приемника. Не будем забывать, что в канале связи присутствуют помехи, которые могут быть вызваны сторонними сигналами и которые тоже вносят свой вклад в шумовую составляющую.

Еще в 1948 г. в своей знаменитой статье «Математическая теория коммуникации» К. Шеннон впервые использовал понятие «бит» (bit — binary digit) для обозначения наименьшей единицы количества информации [18, с. 244; 21, p. 379]. Поскольку за единицу информации принимается бит, то простое отношение сигнал/шум по мощности для современных цифровых систем недостаточно информативно. Применяется другая мера — «сигнал/шум на бит», которая вычисляется как E_b/N_o: где E_b — отношение энергии сигнала, приходящейся на один бит передаваемых данных, к N_o — спектральной плотности мощности шума (СПМ).

Зная соотношение «сигнал/шум на бит», мы можем рассчитать вероятность битовой ошибки, т. е. вероятность того, что принятое значение не совпадает с переданным. При передаче информации вероятность ошибки указывает на частоту появления ошибок, то есть на их возможную долю от общего числа передаваемых бит, а значит, и на возможное искажение информации. Так мы приходим к главному выводу, что именно из соображений минимизации вероятности ошибки и должен выбираться оптимальный маршрут.

Заключение

Алгоритмы маршрутизации для различных сетей очень схожи между собой и используют похожий математический аппарат — это алгоритмы поиска кратчайшего пути. Приняв в качестве метрики (кратчайшего пути) вероятность ошибки, а не дистанцию между исходным пунктом и пунктом назначения, мы получим оптимальные маршруты между участниками сети, обеспечивающие минимальную вероятность ошибки. Минимальная вероятность ошибки в канале обеспечивает не только минимум искажений передаваемой информации, но и высокую пропускную способность канала.

Таким образом, оценивая характеристики сигнала и рассчитывая отношение сигнал/шум в канале, мы можем в любой момент времени определить оптимальный маршрут по критерию минимальной вероятности ошибки.

Выводы

С учетом всего сказанного выше, мы можем сделать вывод о том, что локальные сети способны обеспечить высокоскоростную, надежную, а главное, защищенную от внешнего воздействия и независимую передачу данных между объектами, удаленными на большое расстояние друг от друга. Создание надежных систем связи, соответствующих названным параметрам, является критически важным с точки зрения обеспечения не только информационной безопасности общества как таковой, но и обеспечения общественной безопасности в ситуациях, требующих быстрого и адекватного реагирования.

Литература

1. *Бард А., Зодерквист Я.* Netократия. Новая правящая элита и жизнь после капитализма. СПб. : Стокгольмская школа экономики в Санкт-Петербурге, 2004.
2. *Владимирова Т. Н.* Социальная природа информационной безопасности. М. : АНО Изд. Дом «Науч. Обозрение», 2014.
3. *Зима В. М.* Компьютерные сети и защита передаваемой информации / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. СПб. : Изд-во СПбГУ, 1998.

4. *Зима В. М.* Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. СПб. : БХВ-Петербург, 2003.
5. *Илюшенко В. Н.* Информационная безопасность общества: учеб. пособие для вузов. Томск : Том. гос. ун-т систем управления и радиоэлектроники, 1998.
6. *Кириленко В. П., Алексеев Г. В.* Международная интеграция, демократия и информационная безопасность государства // Управленческое консультирование. 2017. № 3 (99). С. 8–15.
7. *Кириленко В. П., Алексеев Г. В.* Международное право и информационная безопасность государств: монография. СПб. : СпбГИКиТ, 2016.
8. *Кириленко В. П., Алексеев Г. В.* Проблема борьбы с экстремизмом в условиях информационной войны // Управленческое консультирование. 2017. № 4 (100). С. 14–30.
9. *Ковалев А. А., Кудайкин Е. И.* Информационные технологии в обеспечении военной безопасности государства // Управленческое консультирование. 2017. № 5 (101). С. 20–27.
10. *Косов Ю. В., Вовенда Ю. В.* Геополитические концепции информационного противоборства в российской общественной мысли // Управленческое консультирование. 2015. № 10 (82). С. 95–100.
11. *Мак-Люэн Маршалл.* Галактика Гутенберга: Становление человека печатной культуры. Киев : Ника-Центр, 2004.
12. *Маклюэн Г. М.* Понимание Медиа: Внешние расширения человека. М. : КАНОН-пресс-Ц, 2003.
13. *Молдовян Н. А.* Проблематика и методы криптографии. СПб. : Изд-во СПбГУ, 1998.
14. *Морозов А. В.* Организационно-правовое обеспечение информационной безопасности / А. В. Морозов, Т. А. Полякова. М. : РПА Минюста России, 2013.
15. *Полякова Т. А.* Информационная безопасность в условиях построения информационного общества в России: монография. М. : ГОУ ВПО РПА Минюста России, 2007.
16. *Рассолов И. М.* Право и интернет: теоретические проблемы. 2-е изд. М. : Норма, 2009.
17. *Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. М. : ДМК Пресс, 2012.
18. *Шеннон К. Э.* Работы по теории информации и кибернетике / под. ред. Р. Л. Добрушина, О. Б. Лупанова. М. : Изд-во иностранной литературы, 1963.
19. *Хокинг С.* Краткая история времени: От большого взрыва до черных дыр. СПб. : Амфора, 2005.
20. *Dijkstra E. W.* A note on two problems in connexion with graphs // Numer. Math — Springer Science+Business Media, 1959. Vol. 1, Is. 1. P. 269–271.
21. *Shannon C. E.* A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

Об авторе:

Павлов Вячеслав Владимирович, аспирант кафедры государственного и муниципального управления Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация); pavlov1101leti@mail.ru

References

1. Bard A., Zoderkvist J. Nätokraterna — boken om det elektroniska klassamhället (published in English by Reuters/Pearsall UK, 2002. as “Netocracy — The New Power Elite and Life After Capitalism”) Stockholm Text, 2000. (SPb. : Stockholm School of Economics in Saint Petersburg, 2004) (In rus)
2. Vladimirova T. V. Social origins of information security: monography. Moscow : ANO Publishing House “Scientific Review”, 2014. (In rus)
3. Zima V. M. Computer networks and security of data transmission. SPb. : The Publishing House of Saint Petersburg State University, 1998. (In rus)
4. Zima V. M. The security of global network technologies. SPbю : BHV-Petersburg, 2003. (In rus)
5. Iljushenko V. N. Information security of the society: manual for graduate students. Tomsk : Tomsk State University of Control Systems and Radioelectronics, 1998. (In rus)
6. Kirilenko V. P., Alekseev G. V. International Integration, Democracy and Information Security of the State // Administrative consulting [Upravlencheskoe konsul’tirovanie]. 2017. N 3. P. 8–15. (In rus)

7. Kirilenko V.P., Alekseev G.V. International Law and Information Security of the States: monography. SPb. : St.Petersburg State University of Film and Television, 2016. (In rus)
8. Kirilenko V.P., Alekseev G.V. The Problem of Countering Violent Extremism in the Information War // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2017. N 4. P. 14–30. (In rus)
9. Kovalev A.A., Kudaikin E.I. Information Technologies in Military Safety of the State Ensuring // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2017. N 5. P. 20–27. (In rus)
10. Kosov Yu.V., Vovenda Yu.V. The Geopolitical Concept of Information Warfare in the Russian Social Thought // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2015. N 10. P. 95–100. (In rus)
11. McLuhan M. The Gutenberg Galaxy: The Making Typographic Man. Translated from English. Kiev : Nika-Center, 2004. (In rus)
12. McLuhan G.M. Understanding Media: The Extensions of Man. Translated from English. M. : CANON-press-C, 2003. (In rus)
13. Moldavijan N.A. Problems and methods of cryptography. Saint Petersburg : The Publishing House of Saint Petersburg State University, 1998. (In rus)
14. Morozov A.V. Organizational and legal support for information security / F.V. Morozov, T.A. Poljakova. M. : RLA of the Ministry of Justice of Russia, 2013. (In rus)
15. Poljakova T.A. Information security in the context of the development information oriented society in Russia. M. : RLA of the Ministry of Justice of Russia, 2007. (In rus)
16. Rassolov I.M. The law and the Internet: theoretical problems. 2nd edition. Moscow : Norma, 2009. (In rus)
17. Shan'gin V.F. Information security in computer systems and networks. Moscow : DMK-Press, 2012. (In rus)
18. Shannon C.E. Essays on the information theory and cybernetics. Translated from English / ed. by R.L. Dobrushin, O.B. Lupanov. M. : Foreign Languages Publishing House, 1963. (In rus)
19. Hawking S.W. A Brief History of Time: From the Big Bang to Black Holes. SPb. : Amfora, 2005. (In rus)
20. Dijkstra E.W. A note on two problems in connexion with graphs // Numer. Math — Springer Science+Business Media, 1959. Vol. 1. Is. 1. P. 269–271.
21. Shannon C.E. A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

About the author:

Vyacheslav V. Pavlov, Graduate Student of the Chair of the State and Municipal Management of North-West institute of management of RANEPA (St. Petersburg, Russian Federation); pavlov-1101leti@mail.ru