Олег Я. Мадатов
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
ул. Красина, д. 4, г. Краснодар, 350063, Россия
e-mail: oleg_madatov@rambler.ru, https://orcid.org/0000-0003-1956-1791

НЕКОТОРЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНОГО ХРАНЕНИЯ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2018.3.05

Аннотация. В последние годы широкое распространение получили системы удаленного хранения данных, реализуемые с помощью технологий облачного хранения. Их популярность обусловлена существенными преимуществами, предоставляемыми пользователям, по сравнению с другими способами хранения данных и доступа к ним. Действительно, возможность удаленного доступа к информации, размещенной в облачном хранилище, посредством компьютеров, смартфонов, планшетов и других подобных устройств предоставляет возможность ее владельцу в любое время и практически в любом месте (при наличии сети «Интернет») воспользоваться нужными данными.
Однако указанное преимущество несет в себе и определенные риски. Размещение информации на удаленных носителях неминуемо снижает уровень ее защищенности, связанной как с техническими и программными сбоями, так и с противоправной деятельностью других лиц, в результате действий которых возможны утрата, хищение, изменение данных, необходимость предотвращения которых и определяет актуальность проводимого исследования.
Целью исследования является выявление возможных проблем обеспечения информационной безопасности облачного хранения данных и нахождение путей их устранения.
Объектом исследования является уязвимость информационной безопасности наиболее популярных в России облачных хранилищ данных.
Теоретическая база исследования представлена трудами ведущих ученых, таких как И.Ю. Гришин, А.В. Еськов, В.С. Симанков, А.Б. Сизоненко и др.
В процессе проведенного анализа наиболее популярных облачных хранилищ была выявлена проблема, создающая серьезные угрозы информационной безопасности данных, – загрузка файлов на сервер в незашифрованном виде, что создает возможность несанкционированного доступа как на стадии передачи информации, так и в результате неправомерных действий владельцев программного обеспечения или серверов (их сотрудников), оперативников иностранных спецслужб, а также хакерских группировок.
С целью решения указанной проблемы обоснована необходимость разработки специализированного независимого программного обеспечения, позволяющего зашифровать информацию до момента ее передачи с компьютера в облачное хранилище.
Ключевые слова: облачное хранилище данных, конфиденциальность информации, хранение данных, компьютерная безопасность, безопасность хранения данных.
Для цитирования: МАДАТОВ, Олег Я. НЕКОТОРЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНОГО ХРАНЕНИЯ ДАННЫХ. Безопасность информационных технологий, [S.l.], n. 3, p. 45-52, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1139>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.05.

Oleg Y. Madatov
Krasnodar higher military school named after General of the army S. M. Shtemenko,
St. Krasina, d. 4, Krasnodar, 350063, Russia
e-mail: oleg_madatov@rambler.ru, https://orcid.org/0000-0003-1956-1791

Some information security problems of cloud data storage

DOI: http://dx.doi.org/10.26583/bit.2018.3.05

Abstract. Last years the systems of remote data storage based on the Cloud Storage technologies have become widely used. This popularity is explained by its significant advantages for the users as compared to any other technologies of storing and accessing data. Indeed, a remote access of information located in the cloud storage with the help of computers, smartphones, tablets and other similar devices provides an opportunity for its owner to use the data needed at any time and practically everywhere (via the Internet).
However, this advantage has a certain risk. A placement of information on the remote media inevitably reduces its security level. It happens due to both hard- and software failures and any illegal activities. To

prevent the resulting loss, theft or alteration of the data is an important issue discussed below. The aim of the present research is to identify possible information security problems related to the cloud data storage and try to find its solutions. We study the vulnerabilities of information security of the most popular cloud data stores in Russia.
The theoretical basis of the study is given by the works of the leading scientists such as I.Yu. Grishin, A.V. Eskov, V.S. Simankov, A.B. Sizonenko and others.
The analyses of the most popular cloud storages have revealed a problem which creates serious threats to the information security of the data. Namely, file downloads to the server in an unencrypted format opens a possibility of unauthorized access both at the information transfer stage and as a result of illegal actions of software owners or servers employees, operations of foreign intelligence services or hacker groups. We justify that in order to solve this problem it is necessary to develop the specialized independent software which allows encrypting the information before its transfer to the cloud storage.
Keywords: cloud data storage, information privacy, data storage, computer security, data storage security.
For citation: MADATOV, Oleg Y. Some information security problems of cloud data storage. IT Security (Russia), [S.l.], n. 3, p. 45-52, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1139>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.05.

В последнее время наибольшее распространение получили системы удаленного хранения данных (облачное хранение), что обусловлено определенными преимуществами, которые получают пользователи, использующие данный сервис. В частности, они имеют возможность удаленного доступа к собственной информации, размещенного в облачном хранилище, с компьютера, смартфона, планшета и других подобных устройств.

Однако указанное преимущество создает и определенные проблемы. Так, размещение информации в облаке создает определенные риски снижения уровня компьютерной безопасности, связанные с утратой, хищением, изменением личных и/или служебных данных, что и определяет актуальность проводимого исследования.

Изучение научных работ показало, что единого определение понятия облачного хранилища современной наукой не выработано. Существуют различные точки зрения. Так, М.С. Пантелеев и П.И. Авдеев утверждают, что «облачное хранилище данных – это модель хранение данных на многочисленных распределенных серверах. В отличие от модели хранения данных на локальных устройствах или выделенных серверах, эта модель предоставляет в пользование клиентам свои ресурсы (серверы-хранилища) за плату» [1].

Вместе с тем данное определение не учитывает следующие моменты:

во-первых, хранение информации может также осуществляться только на одном удаленном сервере;

во-вторых, ресурсы облачного хранения данных могут предоставляться без оплаты (Яндекс Диск, Google Drive, SkyDrive, Wuala, Dropbox и др.).

Вызывает также сомнения целесообразность указания в конструкции названного определения сравнение облачного хранилища данных с локальными устройствами, что без надобности усложняет понимание просматриваемого явления, не раскрывая его сути.

Кодолов П.А. считает, что «облачное хранилище данных –хранилище данных онлайн, в котором информация пользователя хранится на удаленном сервере (обычно на нескольких распределенных серверах)» [2].

Из указанного определения необоснованно исключен такой важный для пользователя момент, как платность или бесплатность оказываемых услуг. Кроме того, понятие «онлайн» является заимствованным выражением из английского языка и его применение в тексте научного определения видится не вполне корректным.

Более того, указанные авторы понимают под облачным хранилищем модель или виртуальную среду. В тоже время на наш взгляд, облачное хранилище, несмотря на свое название, представляет собой вещь материального мира, в котором хранится информация. Соответственно, данное понимание должно найти свое отражение в указанном понятии.

Проведенное исследование позволило нам сформулировать собственный подход к пониманию сути облачного хранилища данных.

По нашему мнению, облачное хранилище – это часть выделенного дискового пространства на одном или нескольких удаленных серверах, на котором пользователь платно или бесплатно имеет возможность разместить свою информацию и иметь доступ к ней.

Современной наукой разработана определенная классификация облачных хранилищ в зависимости от их принадлежности:

1. Частное облачное хранилище – это вид хранилища, используемого одной организацией.

2. Публичное облачное хранилище – это вид хранилища, используемый широким кругом лиц независимо от принадлежности к какой-либо организации.

3. Клановое облачное хранилище – это вид хранилища, используемый сообществом потребителей из конкретных сфер, имеющихобщие цели и задачи.

4. Гибридное облачное хранилище – это вид хранилища, который использует несколько видов хранилища одновременно для стабилизирования информационного потока между облаками [3].

К преимуществам облачных хранилищ относят [4]:

1. Возможность размещения информации на удаленном сервере (для хранения, использования, восстановления, передачи другим лицам).

2. Бесплатность или низкая стоимость оказываемых услуг по хранению данных.

3. Возможность организации удаленного взаимодействия между юридическими и/или физическими лицами для решения производственных, бытовых или личных задач.

4. Возможность доступа к информации с различных устройств (ПЭВМ, планшеты, смартфоны и др.).

В свою очередь облачное хранилище имеет определенные специфические недостатки, а именно:

1. Возможность безвозвратной потери данных (повреждение или физическое уничтожение носителей и др.). [5]

2. Возможность временных проблем с получением и/или передачей информации (регламентные работы сервера, проблемы с доступом к Internet, не соответствующие требования ПЭВМ и др.).

3. Получение не преднамеренного доступа к информации другими лицами (владелец сервера, разработчик программного обеспечения, специальные службы иностранных государств, «хакеры» и др.). [6]

4. Ограничение доступа к данным при несвоевременной оплате услуг.

В практической деятельности облачные хранилища данных получили широкое распространение. Маркетинговая концепция их продвижения рекламирует облачные хранилища как места, гарантирующие невозможность несанкционированного доступа к информации, хранящейся на серверах компании [7].

Указанного, со слов разработчиков, удалось добиться за счет применения оптимальной политики безопасности. Так, например, компания Dropbox Inc. на официальном сайте dropbox.com заявляет: «Свойство совершенной прямой секретности не позволяет использовать наш закрытый ключ SSL для расшифровки … закрытые ключи безопасно сохраняются» [8]. Компания Microsoft информирует, что имеет возможность «предотвратить утечку секретной информации» [9] с облачного хранилища OneDrive.

Вместе с тем указанные утверждения вызывают обоснованные сомнения. Например, на конференции Black Hat «специалисты компании Imperva показали в Las-Vegace, что получить доступ к чужим файлам в облачном хранилище (будь то Microsoft OneDrive, Dropbox, Google Drive или Box) можно достаточно легко» [10]. Атака состояла из «кражи уникальных токенов, которые генерируются при первом использовании сервиса и для удобства хранятся на пользовательской машине». Тем самым злоумышленник обманывает облачное хранилище, притворяясь настоящим владельцем аккаунта с помощью уникального токена.

С целью определения реального положения дел на основании данных, размещенных в свободном доступе [11], было проведено комплексное исследование безопасности облачных хранилищ, результаты которого представлены в табл. 1.

Таблица 1. Характеристика современных облачных хранилищ

Показатели	Google Drive	SkyDrive (OneDrive)	Dropbox	Box	SuganSync
Система шифрования данных	AES-256	Нет	AES-256	AES-256	AES-256
Обеспечение безопасности доступа к ресурсу	Двухшаговая верификация	Двухшаговая верификация	Защита паролем/ Двухшаговая верификация	Защита паролем/ Двухшаговая верификация	Двухшаговая верификация
Протокол безопасности	TLS 1.2 (AES-128)	TLS 1.2 (AES-128)	SSL/TLS 1.2 (AES-256)	TLS 1.2 (AES-256)	SSL/ TLS 1.2 (AES-256)
Доступ по протоколу	PFS/HSTS	PFS/HSTS	PFS/HSTS	PFS	PFS/HSTS
Шифрование End-to-end	Нет	Нет	Нет	Нет	Нет
Предоставление информации по запросу спецслужб иностранных государств	Да	Да	Да	Да	Да
Предоставление информации по запросу спецслужб РФ	Да	Да	Да	Да	Да
Свободное пространство	5 GB	7 GB	2 GB	5 GB	5 GB
Мин. цена за Премиум	25 GB за 2,49$/мес.	20 GB за 10$/год	50 GB за 9,99$/мес.	25 GB за 9,99$/мес.	30 GB за 4,99/мес.
Макс. цена за Премиум	16 TB за 799,99$/мес.	100 GB 50$/год	100 GB за 19,99$/мес.	50 GB за 19,99$/мес.	100 GB за 14,99$/мес.
Ограничение на размер файлов	10 GB	2 GB	2 GB	100 MB	Нет
Приложения под Windows/Mac	Да	Да	Да	Только для коммерческих предприятий	Да
Приложения под Linux	Нет	Нет	Да	Да	Да
Приложения для iPhone	Да	Да	Да	Да	Да
Приложения для Android	Да	Нет	Да	Да	Да
Приложения для Windows Phone	Нет	Да	Нет	Нет	Да
Web – доступ	Да	Да	Да	Да	Да
Публичное хранение файлов	Да	Да	Да	Да	Да
Частное хранение	Да	Да	Да	Да	Да

файлов					
Совместное редактирование документов	Да	Да	Нет	Да	Нет
Синхронизация с любой папкой	Нет	Нет	Нет	Только с папками предприятия	Да
Интеграция с другими приложениями	Да	Да	Да	Да	Да

Данные таблицы показывают, что в облачных хранилищах Google Drive, Dropbox, Box, SuganSync применяется система шифрования данных AES-256, использующая один из последних симметричных алгоритмов блочного шифрования данных. Вместе с тем она имеет определенные недостатки, которые создают угрозу безопасности хранящейся информации.

Так, например, не может быть обеспечена сохранность информации по естественным каналам ее утечки, которые образуются в результате побочных электромагнитных излучений, появляющихся при обработке информации на ПЭВМ, а также вследствие применения информативных сигналов в линиях электропитания средств вычислительной техники, соединительных линиях вспомогательных технических средств и систем, а также в посторонних проводниках, аналогичной позиции придерживаются авторы S. Khan, S. Parkinson и Y. Qin [12, с. 13].

В результате появляется возможность снятия ключа AES-256, что и было наглядно продемонстрировано компанией Fox-IT. Алгоритм атаки «включал в себя четыре фазы: Аналоговые измерения. Запись радиосигнала. Предварительная обработка. Анализ» [13]. Доказано, что данный алгоритм блочного шифрования не является достаточно надежным для обеспечения сохранности информации в облачном хранилище из-за возможности снятия конфиденциальных данных клиентов облачных платформ.

Более того, облачное хранилище SkyDrive (OneDrive) ОС Windows (компании Microsoft) вообще не осуществляет шифрования хранимой информации, что ставит под сомнение саму целесообразность его использования.

Сравнивая системы безопасности доступа к ресурсам, необходимо отметить, что облачные хранилища Dropbox и Box предоставляют возможность доступа клиентов к своей платформе как с помощью пароля, так и с помощью двухшаговой верификации. С одной стороны это можно расценивать как преимущество для пользователя, но с другой стороны риск несанкционированного доступа к хранилищу существенно возрастает, соответственно, уровень безопасности указанных хранилищ не в полной мере удовлетворяет предъявляемым требованиям.

При анализе протоколов безопасности сделан вывод, что облачные хранилища Google Drive и SkyDrive (OneDrive) применяют морально устаревший 128-битный алгоритм блочного шифрования данных AES-128, дешифрование которого занимает значительно меньше времени, чем его современный аналога.

Облачные хранилища компаний Dropbox и SuganSync до сих пор не смогли полностью перевести свои серверы на современный протокол безопасности TLS. Они предоставляют возможность клиентам использовать также протокол безопасности SSL, который является более ранней версией программы, позволяющей работать с устаревшими устройствами и браузерами. Исследование показывает наличие уязвимости протокола, именуемой POODLE [14], позволяющей несанкционированно завладевать и получать доступ к чужой зашифрованной информации, передаваемой между пользователем и сервером.

Не обеспечивается шифрование информации непосредственно на компьютере пользователя перед ее передачей в облачное хранилище (шифрование End-to-end [15]) ни одним из облачных серверов. Информация, передаваемая по техническим каналам связи,

не зашифрована, соответственно, ее перехват позволяет получать неправомерный доступ к сведениям, в ней содержащимся. Такой перехват может осуществляться как программными, так и аппаратными способами. В случае шифрования информации непосредственно на компьютере пользователя, доступ к ней не имели бы лица, незаконно подключившиеся к каналам связи, а также сотрудники самой компании, что и послужило основанием для отказа от использования названной технологии.

Особое беспокойство вызывает то обстоятельство, что к информации, хранящейся на облачных хранилищах, может быть получен несанкционированный доступ специальными службами иностранных государств, являющимся в том числе нашими вероятными противниками [16]. Так, если получение информации спецслужбами Российской Федерации прямо предусмотрено законодательством России, а ее использование гарантированно ограничивается защитой конституционных прав и свобод граждан, безопасности государства, то доступ к информации иностранных спецслужб будет, безусловно, связан с нарушением наших прав и свобод, созданием угроз территориальной целостности страны и ее военной безопасности.

Таким образом, ни какая информация, представляющая любые виды государственной, налоговой, коммерческой, следственной и иных тайн, ни при каких обстоятельствах не должна размещаться в облачных хранилищах.

Сравнивая между собой экономическую целесообразность использования облачных хранилищ, отметим, что все они предоставляют бесплатный доступ к дисковому пространству, которого вполне достаточно для хранения данных, не представляющих интереса для злоумышленников. Хранение же информации о деятельности предприятий и организаций не целесообразно по причине возможных нарушений безопасности и, соответственно, использовать платный доступ к системе не целесообразно.

На основании проведенного исследования был сделан вывод, что все существующие облачные хранилища не гарантируют конфиденциальности передаваемой информации. Доработка предварительной системы шифрования информации на компьютере также не решит данной проблемы, так как коды шифрования будут содержаться в самом облачном хранилище и, соответственно, будут доступны для использования как злоумышленниками, так и специальными службами.

Единственным решением данной проблемы могло бы стать шифрование информации на компьютере независимой программой шифрования. С учетом требований законодательства Российской Федерации запрета на использование ассиметричных методов шифрования целесообразно разработать программное обеспечение на основании симметричных методов шифрования, например, таких как гаммирование, комбинирование и аналитическое преобразование.

Подводя итог проведённому исследованию, отметим, что использование услуг облачных хранилищ в современном виде не гарантирует конфиденциальности размещенных на них данных. Для решения указанной проблемы предлагается разработать специализированное независимое программное обеспечение, позволяющее зашифровать информацию симметричным методом шифрования до момента ее передачи с компьютера в облачное хранилище.

СПИСОК ЛИТЕРАТУРЫ:

1. Пантелеев М.С., Авдеев П.И. Безопасность в облачных хранилищах // Современные тенденции развития науки и технологий. 2016. № 10-2. С. 45 -4 7.
2. Кодолов П.А. Облачное хранилище данных // Наука, техника и образование. 2016. № 4 (22). С. 51 - 53.
3. Чемеркин Ю.С. Облачные вычисления как инструмент обработки конфиденциальной информации // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2012. № 14 (94). С. 53 - 65.
4. Михайлова О.П. Актуальность использования облачных технологий // Профессиональные коммуникации в научной среде - фактор обеспечения качества исследований материалы II Всероссийской научно-практической конференции с зарубежными участниками. Казанский национальный исследовательский технический университет им. А.Н. Туполева, Альметьевский филиал. 2016. С. 43 - 46.
5. Лященко Ю.В., Багаева А.П. Преимущества и недостатки облачных технологий // Актуальные проблемы авиации и космонавтики. 2014. Т. 1, № 10. С. 380 – 381.
6. Леонов В. GoogleDocs, WindowsLive и другие облачные технологии // Эксмо - Пресс, 2012, с. 304.
7. Maksutov A.A., Kutepov S.V., Hrapov A.S. Efficient processing and storage of data on untrusted cloud storage services // Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, ElConRus 2017 2017. С. 496-500.
8. Что происходит за кулисами: обзор архитектуры [электронный ресурс]: https://www.dropbox.com/business/trust/security/architecture (Дата обращения: 21.04.2018 г.)
9. Защита информации [электронный ресурс]: https://www.microsoft.com/ru-ru/security/information-protection (Дата обращения: 15.04.2018 г.)
10. Исследователи нашли способ проникнуть в хранилища Dropbox, OneDrive, Box, Drive [электронный ресурс]: https://xakep.ru/2015/08/07/man-in-the-cloud-attack/ (Дата обращения: 18.04.2018 г.)
11. 20 лучших облачных хранилищ данных [электронный ресурс]: http://www.internet-technologies.ru/articles/20-luchshih-oblachnyh-hranilisch-dannyh.html (Дата обращения: 22.04.2018 г.)
12. Khan S., Parkinson S., Qin Y. Fog computing security: a review of current applications and security solutions // Journal of Cloud Computing: Advances, Systems and Applications. 2017. P. 22 DOI 10.1186/s13677-017-0090-3
13. Ключ AES-256 сняли с расстояния 1 метр по электромагнитному излучению компьютера [электронный ресурс]: https://geektimes.ru/post/290411/ (Дата обращения: 23.04.2018 г.)
14. Давлетшина А.М., Рыбкин А.С., Елисеев В.Л. Особенности использования технологий VPN и SSL/TLS // Защита информации. Инсайд. 2016. № 6 (72). С. 64-70.
15. Мазунина Е.С., Кротова Е.Л. Сквозное шифрование // Научное сообщество студентов Сборник материалов IX Международной студенческой научно-практической конференции: в 2 томах. ФГБОУ ВПО «Чувашский государственный университет им. И.Н. Ульянова»; Харьковский национальный педагогический университет имени Сковороды; Актюбинский региональный государственный университет им. К. Жубанова; ООО «Центр научного сотрудничества «Интерактив плюс». 2016. С. 48-50.
16. Гребенников Н. Киберугрозы сегодня: предупрежден – значит, вооружен // Первая миля. 2017. № 4 (65). С. 76-78.

REFERENCES:

[1] Panteleev M. S., Avdeev P. I. Security in cloud storage. Modern trends in the development of science and technology. 2016. No. 10-2. P. 45-47. (in Russian).
[2] Kodolov p. A. cloud data storage. Science, technology and education. 2016. № 4 (22). P. 51-53. (in Russian).
[3] Chemerkin Y. S. Cloud computing as a tool for handling confidential information]. Vestnik RGGU. Series: documentary and archival science. Informatics. Information security and information security. 2012. № 14 (94). P. 53-65. (in Russian).
[4] The Relevance of the use of cloud technologies. Professional communications in the scientific environment - a factor in ensuring the quality of research materials II all-Russian scientific and practical conference with foreign participants. Kazan national research technical University. A. N. Tupolev, Almetyevsk branch. 2016. P. 43-46. (in Russian).
[5] Lyashchenko, Yu., Bagaeva, A. P. the Advantages and disadvantages of cloud computing. Actual problems of aviation and cosmonautics. 2014. Vol. 1, No. 10. P. 380 – 381. (in Russian).
[6] Leonov V. GoogleDocs, WindowsLive and other cloud technologies. Eksmo - Press, 2012, p. 304. (in Russian).
[7] Maksutov A. A., Kutepov S. V., Hrapov A. S. Efficient processing and storage of data on untrusted cloud storage services. Processing of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, ElConRus 2017 2017. P. 496-500.

[8] What happens behind the scenes: architecture overview [electronic resource]: https://www.dropbox.com/business/trust/security/architecture (date accessed: 21.04.2018 G.) (in Russian).
[9] Data protection [electronic resource]: https://www.microsoft.com/ru-ru/security/information-protection (date accessed: 15.04.2018 G.) (in Russian).
[10] Researchers have found a way to get into Dropbox, OneDrive, Box, Drive [electronic resource]: https://xakep.ru/2015/08/07/man-in-the-cloud-attack/ (accessed: 18.04.2018 G.) (in Russian).
[11] Top 20 cloud storage services [electronic resource]: http://www.internet-technologies.ru/articles/20-luchshih-oblachnyh-hranilisch-dannyh.html (date accessed: 22.04.2018 G.) (in Russian).
[12] Khan S., Parkinson S., Qin Y. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing: Advances, Systems and Applications. 2017. P. 22 DOI 10.1186/s13677-017-0090-3.
[13] Key AES-256 removed from a distance of 1 meter by electromagnetic radiation of the computer [electronic resource]: https://geektimes.ru/post/290411/ (date of circulation: 23.04.2018 g.) (in Russian).
[14] Davletshina A. M., Rybkin A. S., Eliseev V. L. peculiarities of the use of VPN technologies and SSL/TLS//. Insider trading. 2016. No. 6 (72). P. 64-70. (in Russian).
[15] Mazunina E. S., Krotova E. L. end-to-End encryption. Scientific community of students proceedings of the IX international student scientific and practical conference: in 2 volumes. Fgbou HPE "Chuvash state University. I. N. Ulyanov"; Kharkiv national pedagogical University named after Skovoroda; Aktobe regional state University. K. Zhubanova; LLC "center for scientific cooperation "Interactive plus". 2016. P. 48-50. (in Russian).
[16] Grebennikov N. Cyber threats today: warned-means armed. The first mile. 2017. № 4 (65). P. 76-78. (in Russian).

Поступила в редакцию - 26 мая 2018 г. Окончательный вариант – 23 августа 2018 г.
Received – May 26, 2018. The final version – August 23, 2018.