УДК 11.15.25
DOI: 10.21209/2227-9245-2017-23-7-86-90

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АСПЕКТЕ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ

INFORMATION SECURITY IN THE ASPECT OF SECURE ELECTRONIC DOCUMENT MANAGEMENT IN INFORMATION SYSTEMS OF MUNICIPALITIES

А. Н. Кухарский, *Забайкальский государственный университет, г. Чита*
kukharskijjartjom@yandex.ru

A. Kukharsky, *Transbaikal State University, Chita*

Статья посвящена актуальным вопросам информационной безопасности местного самоуправления в Российской Федерации и анализу трансформации угроз информационным системам в области местного самоуправления. Автор акцентирует внимание на том, что защищенность электронного документооборота местного самоуправления недостаточная, что приводит к необходимости изменения информационных систем муниципалитетов. Рассматриваются угрозы местного самоуправления в информационной сфере: несанкционированный доступ, хакерские атаки, нарушение секретности, целостности и доступности информации. Проведенный анализ свидетельствует о том, что трансформация информационных систем муниципальных образований Российской Федерации требует контроля со стороны государственной системы защиты информации. Особое внимание уделяется анализу опыта России и США в области больших вычислительных мощностей широкого распространения, шифр PGP. В заключение автор указывает на то, что система электронного документооборота с применением криптографических систем защиты в муниципальных образованиях должна являться частью общегосударственной системы документооборота

Ключевые слова: *информация; информационная безопасность; государство; муниципальные образования; электронный документооборот; защита информации; США; Россия; информационные системы управления; криптографическая система*

The article is devoted to topical issues of information security of local government in the Russian Federation and analysis of the transformation of the threats to information systems in the field of local government. The author focuses on the fact that the security of electronic document flow of local self-government is insufficient, which leads to the necessity of changing the information systems of municipalities. The threats to local self-government in the field of information: unauthorized access, hacking, violation of privacy, integrity and availability of information are discussed. The analysis suggests that the transformation of information systems of municipal formations of the Russian Federation requires control of the state system of information protection. Special attention is paid to the analysis of experience of Russia and the USA in the field of high computing power, widespread cipher PGP. In conclusion, the author points to the fact that the system of electronic document circulation with use of cryptographic protection systems in the municipalities should be a part of megasuperstar document management system

Key words: *information; information security; state; municipalities; electronic document management; information security; USA; Russia; management information system; cryptographic system*

Введение. Актуальность исследования защиты информации от постороннего доступа и нежелательного воздействия на нее возникла с той поры, когда начали раз-

виваться телекоммуникационные технологии. Проблема информационной безопасности актуальна как для государственных органов власти, так и для муниципальных образований любого государства. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцу в лице государственных и муниципальных органов получить какой-либо выигрыш. С переходом на использование технических средств связи информация подвергается воздействию случайных процессов (неисправностям и сбоям оборудования, ошибкам операторов и т.д.), которые могут привести к ее разрушению, изменению, а также создать предпосылки к доступу к ней посторонних лиц [5]. Поэтому значимость информационной безопасности и защищенного электронного документооборота возрастает в условиях информационного общества.

Методология и методика исследования. Автором использовались нормативный, системный, сравнительный, институциональный и информационный методы исследования. Особое значение имеет информационный, или технический метод, который проанализирован с точки зрения информационной безопасности (работы В. В. Бордюже [3], Е. Н. Донской [6], В. А. Семененко [8], В. И. Ярочкина [10]).С появлением сложных автоматизированных систем управления, связанных с автоматизированным вводом, хранением, обработкой и выводом информации, проблемы ее защиты приобретают еще большее значение [7]. Главная причина незащищенного и неразвитого электронного документооборота — «человеческий фактор». Для работы в данной сфере требуются умение работать с компьютером, специализированные знания по программному обеспечению при минимуме специалистов. Подобных кадров в муниципальных образованиях зачастую нет. По данной причине электронный документооборот остается незащищенным без соответствующей подготовки кадров, а также без насыщенности компьютерами и оргтехникой в муниципальных образованиях [4; 9].

Перечисленные проблемы глобальны в том смысле, что они общие для любой разновидности муниципального образования. Они не способны остановить развитие, а могут только оттянуть сроки широкого применения безопасного электронного документооборота. Кроме них есть специфическая проблема, которая способна не только затормозить, но и сделать невозможным электронный документооборот в рамках современного состояния муниципальных образований. Это проблема защиты информации при электронном документообороте, которая требует государственной информационной политики, о чем утверждает Т. Е. Бейдина: «Необходимость информационной прозрачности деятельности органов власти... в условиях развития технологий электронного правительства» [1. С. 38].

Результаты исследования и область их применения. Электронный документооборот значительно больше уязвим, чем его бумажный предшественник. С файлами значительно легче можно сделать копию, внести в него несанкционированные изменения, изготовить фальшивый документ. Имея сравнительно недорогое оборудование, можно производить те же действия и с каналом связи. Поэтому рассмотрим проблему защиты информации подробнее [11]. В этой связи выделим три вида угроз информации — секретность, целостность и доступность.

Защита данных от угроз первого вида осуществляется в большей мере методами стеганографии и криптографии. Стеганография занимается аспектом сокрытия от злоумышленника перечного факта передачи сообщения. В настоящее время— это не только классические симпатические чернила. В приложении к компьютерным технологиям — это дополнительные биты в файлах, не портящие качества изображения. Определить сокрытое таким образом сообщение, не зная метода сокрытия, практически невозможно. В этом файле можно скрыть количество информации, превышающее по размеру оригинальный файл. Общим недостатком стеганографических

методов защиты информации является проблема сохранения тайны метода сокрытия. Для защиты информации в муниципалитетах при электронном документообороте стеганография не сможет найти широкого применения, так как требует специальной подготовки, которая не преподается в рамках специальности «Государственное, муниципальное управление».

Криптография занимается проблемой сокрытия текста сообщения, делая его нечитаемым. При этом допускается, что злоумышленник имеет информацию не только самого факта передачи сообщения, но и само сообщение, возможно, его приблизительный или даже точный текст. Также допускается знание его метода шифрования. Втайне от злоумышленника должен оставаться секретный параметр шифрования – ключ. Секретность в этой сфере деятельности столь велика, что большая часть граждан не имеют представление об этих методах.

Возможный выход из данной ситуации нашли и уже применяют на практике США. Разработаны и разрешены к применению только такие шифры, для вскрытия которых требуются большие вычислительные мощности, имеющиеся в распоряжении только у Агентства национальной безопасности США. Примером может служить приобретший широкое распространение шифр PGP. Этот шифр практически безукоризнен в теории, но реализуется так, что, имея требуемые вычислительные мощности, можно читать, изменять или подделывать любые передаваемые сообщения.

В большей части документооборота муниципальных образований просто не требуется криптографическая защита при хранении и (или) передаче. Поэтому выход из данной ситуации видится в организации в муниципальных образованиях двух или нескольких параллельных систем электронного документооборота. Криптографическая защита может полностью отсутствовать, либо могут применяться те же методы, что и в США. И только в политико-финансовых сферах требуется применение стойких к взлому криптосистем. Подобные системы давно разработаны, проверены и сертифицированы. Их широкое внедрение в электронный документооборот – дело ближайшего будущего.

Защита целостности электронного документооборота требуется всегда, независимо от применения шифрования или его отсутствия. В общем случае цели целостности делятся на задачи защиты от несанкционированного изменения, подлога, пропажи. Первыми двумя аспектами занимается криптография.

Для защиты документа от угрозы применяются специальные имитоприставки, которые строятся с применением хеш-функций – это разновидность контрольной суммы, обладающая теми свойствами, что для нее нельзя иначе, кроме как перебором, вычислить прообраз и очень трудно подобрать два разных значения с совпадающими функциями. Обычно для вычисления имитоприставок применяют схемы блочного шифрования либо используют схемы на основе решения сложных математических задач. Этим достигается необычайная трудность изменения документа при сохранении неизменной имитоприставки документа.

Для защиты от информационной угрозы разработаны криптографические схемы, известные как цифровая подпись, основанные на криптографии с открытым ключом. Суть цифровой подписи – это несколько целых чисел, два из которых это хеш-сумма и открытый ключ, связанные между собой некоторой математической зависимостью; при этом проверить эту зависимость легко, а построить эти числа можно только зная секретный параметр (секретный ключ). Таким образом, цифровая подпись решает ещё одну задачу – подписавший документ не сможет впоследствии отказаться от своей подписи, так как для подделки цифровой подписи нужно знание секретного ключа, известного только ему. Разработаны различные схемы цифровой подписи; наиболее известной является схема Эль-Гамаля. Необходимо отметить, что цифровая подпись чаще всего используется на федеральном и региональном уровнях, но достаточно редко используется в муниципалитетах Российской Федерации.

Следует отметить, что сама по себе цифровая подпись не гарантирует подлинности документа, так как злоумышленник может использовать любой секретный ключ, и при этом математическая зависимость компонентов цифровой подписи сохранится. Чтобы решить данную проблему, требуется заранее передать всем абонентам открытый ключ по защищенному каналу связи.

На отсутствии этой компоненты связи основан способ чтения сообщений, с помощью криптосистемы PGP, не имея при этом достаточных вычислительных мощностей. Злоумышленнику для этой цели требуется перехватить пакет данных, содержащий открытый ключ PGP, и подменить его своим ключом.

Решение проблемы пропажи документа по большей части лежит вне пределов шифрования. При хранении документов необходимо регулярно создавать резервные копии с носителей информации, дублировать, вести учёт поступающих в муниципалитет документов. При передаче документа по каналам связи требуются защищённые, специальные протоколы передачи информации, которые контролируют целостность передачи путем посылки отправителю подтверждения о доставке.Передача информации возможна разными маршрутами, пока не удостоверятся, что к получателю она доставлена в целости и сохранности. Если злоумышленник контролирует линию связи муниципалитета (а этот аспект не следует исключать), то он может не пропустить нужный документ, но послать в ответ подтверждение о доставке. Поэтому подтверждение обязательно следует удостоверять цифровой подписью получателя.

Третий уровень угроз, встречаемый в муниципалитетах, — угрозы доступности информации — основывается в отказе санкционированному доступу к информации со стороны информационной системы. Не следует сравнивать данный аспект с проблемой пропажи документа из-за кажущегося формального сходства. Во втором случае пользователь имеет доступ к информации, однако она может фильтроваться злоумышленником. При отказе в обслуживании легальный пользователь по тем или иным причинам полностью отвергается системой. Способов создать ситуацию отказа в обслуживании достаточно много, начиная от многократных попыток входа в систему от имени пользователя до блокировки его учетной записи, заканчивая применением хакерских атак на сервер. Этот уровень угроз не столь опасен для муниципалитетов своими последствиями как угрозы секретности или целостности.

Выводы. В заключение следует отметить существенный момент. Система электронного документооборота с применением криптографических систем защиты в муниципальных образованиях должна являться частью общегосударственной системы документооборота. Учитывая её уязвимость к следующим угрозам: секретности, целостности и доступности информации, необходимо, чтобы муниципальная информационная безопасность обязательно контролировалась государственной системой защиты информации.

Список литературы

1. Бейдина Т. Е. Государственная информационная политика в Забайкальском крае // Власть. 2014. № 7. С. 36.

2. Бейдина Т. Е. Оценка политической власти и политической системы в субъекте РФ // Власть. 2013. № 5. С. 22.

3. Бордюже В. В., Белозеров А. В., Софьина И. В. Информационная безопасность. Пермь: Пермский центр научно-технической информации, 2009. С. 276.

4. Гафнер В. В. Информационная безопасность. Ростов-н/Д.: Феникс, 2015. 324 с.

5. Генне О. В. Основные положения стеганографии // Защита информации Конфидент. 2001. № 3. С. 20–25.

6. Донская Е. Н., Панько Ю. В. Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления // Молодой ученый. 2014. № 8. С. 453–457.

7. Крупский А. Ю., Феоктистова Л. А. Информационный менеджмент. М.: Дашков и К°, 2008. 80 с.
8. Семененко В. А. Информационная безопасность. М.: МГИУ, 2010. 277 с.
9. Черноусов М. В. Совершенствование механизмов информационной открытости в системе муниципального управления // Вестник Самарского муниципального института управления. 2010. № 2 (13).
10. Ярочкин В. И. Информационная безопасность. М.: Акад. Проект, 2008. 544 с.
11. Ferdinand P. TheInternet, Democracy and Democratization// InDemocratization.2000. Vol.7. No. 1. P. 6.

References

1. Beydina T. E. Vlast (Power), 2014,no. 7,p. 36.
2. Beydina T. E. Vlast (Power), 2013,no. 5,p. 22.
3. Bordyuzha V. V., Belozerov A. V., Sofina I. Informatsionnaya bezopasnost [Information security]. Perm: Perm Center for Scientific and Technical Information, 2009,p. 276.
4. Gafner V. V. Informatsionnaya bezopasnost [Information security]. Rostov-n/D.: Feniks, 2015. 324 p.
5. Gennet O. V. Zashhita informatsii Konfident(Protection of information Confident), 2001, no. 3, pp. 20–25.
6. Donskaya E. N., Panko Yu. V. *Molodoy ucheny* (Young Scientist), 2014,no. 8, pp. 453–457.
7. Krupsky A. Yu., Feoktistova L. A. *Informatsionny menedzhment* [Information management]. Moscow: Dashkov and Co, 2008. 80 p.
8. Semenenko V. A. *Informatsionnaya bezopasnost* [Information security]. Moscow: MSIU, 2010. 277 p.
9. Chernousov M. V. *Vestnik Samarskogo munitsipalnogo instituta upravleniya* (Bulletin of the Samara Municipal Management Institute), 2010, no. 2 (13).
10. Yarochkin V. I. *Informatsionnaya bezopasnost* [Information Security]. Moscow: Acad. Project, 2008. 544 p.
11. Ferdinand P. *In Democratization* (In Democratization), 2000,vol. 7,no. 1, p. 6.

Коротко об авторе ***Briefly about the author***

Кухарский Артем Николаевич, стажер-исследователь кафедры «Государственное, муниципальное управление и политика», Забайкальский государственный университет, г. Чита, Россия. Область научных интересов: политические науки, государственное управление, информационная безопасность
kukharskijjartjom@yandex.ru

Artem Kucharsky, trainee researcher, State, Municipal Management and Policy department, Transbaikal State University, Chita, Russia. Sphere of scientific interests: political science, public administration, information security

Образец цитирования

Кухарский А. Н. Информационная безопасность в аспекте защищенного электронного документооборота в информационных системах муниципальных образований // Вестн. Забайкал. гос. ун-та. 2017. Т. 23. № 7. С. 86–90. DOI: 10.21209/2227-9245-2017-23-7-86-90.

Kukharsky A. Information security in the aspect of secure electronic document management in information systems of municipalities // Transbaikal State University Journal, 2017, vol. 23,no. 7, pp. 86–90. DOI: 10.21209/2227-9245-2017-23-7-86-90.

Дата поступления статьи: 07.07.2017 г.
Дата опубликования статьи: 31.07.2017 г.