ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо використання і зберігання електронної інформації в сучасному інформаційному суспільстві.

У публікації «Возможности для использования блокчейна в архивах» розповідається про використання блокчейна, для підтвердження дійсності сертифікатів електронних підписів.

У публікації «Презентация к докладу доктора Хрвое Станчича «Возможности для использования блокчейна в архивах»» наведено матеріали презентації.

У публікації «Россия создала национальное облачное хранилище» розповідається про хмарне сховище інформації Росії та його призначення.

У публікації «Нидерланды отказались от антивирусов «Касперского» из соображений безопасности» розповідається що уряд Нідерландів прийняв рішення про відмову від антивірусів Касперського з метою забезпечення національної безпеки.

У публікації «Рік після атаки вірусу Petya: що змінилося в кібербезпеці України» розповідається про зміни в Україні після атаки вірусу Petya.

У публікації «Новая кибератака на Украину: что такое вирус VPNFilter и как с ним бороться» розповідається про вірус VPNFilter та як з ним боротися.

У публікації «Обеспечение безопасности информационных ресурсов предприятия» розповідається що тільки об'єднання зусиль фахівців різних напрямів може створити ефективну систему захисту.

У публікації «Управление метаданными документов постоянного срока хранения: Как быть, если метаданные, требуемые для передачи документов на архивное хранения, хранятся отдельно от самих документов?» розповідається що до метаданих, які передаються на архівне зберігання разом з електронними документами постійного терміну зберігання, мають бути встановлені ті ж терміни зберіганні і дії, що і для документів, які вони описують.

У публікації «Росархив выложил проект «Типовых функциональных требований к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов»» розповідається про розміщення на сайті Росархіву проекту вказаного документу, наведено декілька коментарів.

У публікації «Чехия: Краткий отчет о международном семинаре «Архивы в электронную эпоху» AiDA-2018» наведено інформацію про питання що було розглянуто на семінарі.

ВОЗМОЖНОСТИ ДЛЯ ИСПОЛЬЗОВАНИЯ БЛОКЧЕЙНА В АРХИВАХ

Источник: YouTube https://www.youtube.com/watch?v=vq9OIqD6RMc
Автор: Наташа Храмцовская

Предлагаю вниманию читателей статью профессора кафедры информационно-коммуникационных наук факультета гуманитарных и социальных наук университета Загреба, Хорватия, д-ра Хрвое Станчича.

ы

Хрвое Станчич (в центре) на конференции в Казани, апрель 2018 года

Аннотация

Для архивов обеспечение долговременной сохранности подписанных усиленными электронными подписями или снабжённых электронными печатями электронных документов представляет собой проблему. Помимо хорошо известных подходов к обеспечению сохранности подобных документов, таких, как сохранение возможности перепроверять усиленные электронные подписи, «снятие» подписей и документирование сведений о подписях в метаданных, существуют и другие варианты, такие, как перенос документов в доверенную базу данных или же регистрация факта действительности электронной подписи в блокчейне. Автор основное внимание уделяет последнему варианту и представляет модель TrustChain – решение на основе блокчейна, обеспечивающее сохранение сведений о действительности сертификатов (Validity Information Preservation, VIP) - разработанную в рамках исследовательского проекта InterPARES Trust.

Введение

Сегодня электронные документы могут создаваться двумя способами – либо в результате оцифровки существующих бумажных документов, либо

изначально создаваться в электронном виде. Оцифровка в широком смысле представляет собой преобразование аналогового сигнала в соответствующую электронно-цифровую форму, а в более узком смысле – преобразование различных материалов в электронную форму, путем превращения их в двоичный код, сохраняемый в виде компьютерного файла (Croatian Encyclopedia, Miroslav Krleža Institute of Lexicography, 2017). Оцифровка приводит к разделению деятельности по обеспечению долговременной сохранности на два направления: сохранение информационного контента т.е. зафиксированной в документе информации, и сохранение физического объекта – носителя информации. Информационный контент оцифровывается и сохраняется отдельно от физического объекта (Stančić, Digitization of documents, 2000).

Важно отметить, что у каждого сохраняемого в электронном виде документа должны оставаться неизменными свойства аутентичности, надежности, целостности и пригодности к использованию (ISO 15489-1:2016, Information and documentation – Records management – Part 1: Concepts and principles, 2016). Доверие к документу опирается на его точность, надежность и аутентичность (InterPARES Trust Terminology Database).

Архивирование и обеспечение долговременной сохранности представляют собой уникальную проблему из-за долгосрочного характера такого рода деятельности. Проблема обеспечения долговременной сохранности и поддержания электронной информации может быть истолкована как сохранение документов таким образом, чтобы не устарела та технология, на которой они основаны. Электронные объекты требуют постоянного и непрерывного обслуживания и зависят от сложной экосистемы, включающей оборудование, программное обеспечение, стандарты и правовые нормы, которые постоянно меняются, исправляются или заменяются. Электронные документы, по сравнению с аналоговыми, в большей степени подвержены риску морального устаревания и деградации, что в первую очередь связано с быстрыми темпами развития информационных технологий. Для долговременной сохранности электронных документов требуется куда большее, чем сохранение компьютерных файлов – задача заключается в том, чтобы поддерживать доступ к контенту документов, одновременно обеспечивая сохранение их ключевых свойств.

Документы, подписанные усиленными электронными подписями

Проблема криптосистемы открытых ключей – это проблема защищённой связи между ключом и физическим лицом, т.е. это остается открытым вопрос о личности человека, который электронно подписывает документ. Успешная проверка подписи не означает, что документ был подписан именно указанным лицом, а говорит лишь о том, он был подписан с использованием закрытого (секретного) ключа, соответствующего данному открытому ключу. Таким образом, в криптосистеме открытых ключей существует лишь уверенность в успешном обмене ключами, однако истинности личности подписанта доверять нельзя.

Эта проблема решается с помощью инфраструктуры открытых ключей (public key infrastructure, PKI), в рамках которой доверенная третья сторона (удостоверяющий центр, УЦ) удостоверяет личность человека и его связь с парами открытых и закрытых ключей (*в терминологии российского законодательства, ключей подписания и проверки – Н.Х.*). Эта технология основана на рекомендациях Международного союза электросвязи X.509, впервые опубликованных в 1988 году, и стандарте Интернета RFC 3280, вышедшем в 2002 году. Ценность такой системы заключается в ее гибкости при предоставлении услуг и приложений для идентификации, аутентификации, электронных цифровых подписей, а также для обеспечения безопасности и секретности. Инфраструктура PKI фактически представляет собой систему электронных сертификатов (*в российской терминологии – сертификатов ключа проверки электронной подписи – Н.Х.*), а также сертификационных и регистрационных услуг, которые обеспечивают проверку личности пользователя, – и это её основная цель.

Комментарий: *Речь здесь идёт о следующих документах:*

- *МСЭ-Т X.509 «Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов» (Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks). Текущей является 8-я редакция, опубликованная в октябре 2016 года, см.* http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509 ;
- *RFC 5280 (с исправлениями согласно RFC 6818) «Описание сертификатов и списков отозванных сертификатов для X.509/PKI-инфраструктуры Интернет-сети» (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), см.* https://tools.ietf.org/html/rfc5280 *, на русском языке* - https://rfc2.ru/5280.rfc/55

Инфраструктура PKI может поддерживать:

- проверку личности;
- целостность информации;
- более безопасные процессы обмена данными;
- публичный доступ к государственным и другим электронным услугам;
- возможность подавать различные документы в электронном виде;
- защищенный обмен информацией с сотрудниками, находящимися в удаленных местах.

Инфраструктура PKI включает все необходимые компоненты для управления (включая выдачу, проверку и отзыв) открытыми ключами и сертификатами (а также для их хранения и обеспечения долговременной сохранности). Она также обеспечивает защищённую аутентификацию участников информационного обмена, обмен документами с возможностью шифрования, электронное подписание одной или несколькими сторонами и ведение реестра открытых ключей в форме электронных сертификатов.

Для надёжной идентификации личности подписанта необходимо использовать электронный сертификат. В сертификате открытый ключ

пользователя хранится вместе с его идентификационными данными, и эта информация подписывается Удостоверяющим центром - доверенной третьей стороной. Электронные сертификаты обычно выдаются на срок от двух до пяти лет, поскольку чем дольше срок действия, тем больше уязвимость к потенциальным атакам из-за ослабления криптографических алгоритмов вследствие роста вычислительных мощностей. Например, в Хорватии национальные удостоверения личности раньше выдавались на срок в десять лет. В настоящее время эти удостоверения, изготавливаемые на основе встроенных чипов и содержащие личные усиленные электронные подписи, выдаются сроком на пять лет - именно по указанным выше причинам.

Из-за всего этого в ситуации, когда документ подписывается усиленной электронной подписью и попадает в архивы на краткосрочное или длительное хранение, очень короткий срок действия электронных сертификатов может стать проблемой. Согласно Бланшетту (Blanchette, 2006), электронные архивы в таком случае могут:

- попытаться обеспечить долговременную сохранность усиленных электронных подписей (*под этим понимается сохранение возможности перепроверить усиленные электронные подписи – Н.Х.*);
- «снять» их, либо записать сведения об электронных подписях в метаданные.

Если электронные архивы попытаются обеспечить сохранность подписей, им придётся полагаться на процедуры повторного подписания (переподписания) или повторного проставления отметок времени, используя, например, так называемые «архивные» отметки времени, описанные европейским стандартом ETSI EN 319 102-1 версия 1.1.1 (май 2016 г.) «Электронные подписи и инфраструктуры – Процедуры создания и проверки усиленных электронных подписей AdES. Часть 1: Создание и проверка» (Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation).

Однако использование такого подхода будет означать, что придётся отслеживать истечение срока действия электронного сертификата (сертификатов) для каждого подписанного усиленными электронными подписями документа архива, и проводить его переподписание либо проставление новой отметки времени до истечения срока действия соответствующих сертификатов, – что может со временем и/или в крупных электронных архивах стать вычислительно-интенсивной задачей.

С другой стороны, в случае «снятия» усиленных электронных подписей (*что обычно означает не столько удаление подписей, сколько отказ от их последующей перепроверки – Н.Х.*) документы теряют один из технических элементов, который имеет решающее значение для сохранения их аутентичности. Такой выбор будет скорее говорить о том, что электронный архив не был готов или не хотел обеспечивать сохранность подписанных усиленными электронными подписями документов.

Мой комментарий: *Я бы не согласилась со столь жёсткой оценкой данного подхода. Очень многое, я считаю, зависит от контекста – от вида документов, их содержания, от деловых процессов, в которых они участвуют, от целей применения подписей, от того, как организована передача документов в архив и какая под это разработана нормативно-правовая база, и т.д. В ряде случаев «снятие» усиленной электронной подписи (даже без фиксации сведений о ней в метаданных) может оказаться вполне разумным подходом.*

Третий вариант – фиксация в метаданных сведений об усиленной электронной подписи, т.е. о её наличии и результате проверки – по-прежнему требует наличия доверенной третьей стороны для аутентификации метаданных, и доверенного электронного хранилища для того, чтобы вопрос о доверии решать не для каждого отдельного документа, а на уровне электронного архива.

Тем не менее, исследование, проведенное в рамках проекта InterPARES Trust, показывает, что существует и четвертый вариант – запись в блокчейн сведений о действительности сертификатов.

Мой комментарий: *С моей точки зрения, есть и иные подходы к решению проблемы, которые здесь не упомянуты. Отмечу возможность создания государственного реестра, в котором сведения о подписанных должностными лицами государственных органов электронных документах могли бы фиксироваться в момент их создания или близко к нему (что вернуло бы нас, на новом уровне технологий, к первоначальной идее регистрационной системы).*

TrustChain – блокчейн-решение, обеспечивающее сохранение сведений о действительности сертификатов

В рамках выполняемого в рамках программы InterPARES Trust исследования «Модель доверия к документам, подписанным усиленными электронными подписями, снабженными отметками времени и/или электронными печатями» (Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records - TRUSTER Preservation Model) (Stančić et al., 2018), было промоделировано решение TrustChain для сохранения сведений о действительности подписей, отметок времени и печатей.

Идея, лежащая в основе решения TrustChain (Bralić, Kuleš and Stančić, 2017), заключается в том, чтобы, в идеале, сформировать международный альянс архивных учреждений, участвующих в качестве узлов в архивной блокчейн-системе. Когда документ поступает на хранение в любой из электронных архивов участвующих в системе учреждений, проверяется достоверность соответствующего электронного сертификата. Проверка выполняется всеми участвующими узлами или их квалифицированным большинством (50% + 1), которые затем представляют свои голоса (т.е. подтверждения действительности сертификатов). Этот процесс следует принципу распределенного консенсуса. Действительность сертификата проверяется с использованием списка отозванных сертификатов (certificate revocation list, CRL) или интернет-протокола проверки статуса сертификата

(online certificate status protocol, OCSP), чтобы определить, не был ли сертификат отозван. Затем информация о действительности сертификата, наряду с итогами голосования узлов, сохраняется в блоке и вычисляется итоговое значение хеша (т.е. хеш блока верхнего уровня). Впоследствии этот хеш используется при создании следующего блока, тем самым формируется цепочка блоков, или «блокчейн». Когда блок «опечатан», он распространяется по всем учреждениям-участникам, т.е. записывается в распределенный реестр. Этот процесс показан на рисунке 1.

Впоследствии любое изменение в документе можно будет обнаружить, поскольку в этом случае зарегистрированный хеш и вновь вычисленное значение хеша не совпадут. Кроме того, будет обнаружено и изменение информации в любом из учреждений, поскольку все экземпляры распределенного реестра должны быть идентичными.

Важно то, что в блокчейне регистрируются только хеши документов, а сохранность самих документов по-прежнему должны обеспечивать электронные архивы. Блокчейн используется только для сохранения подтверждающей действительность сертификата информации и хеш-значения соответствующего документа.

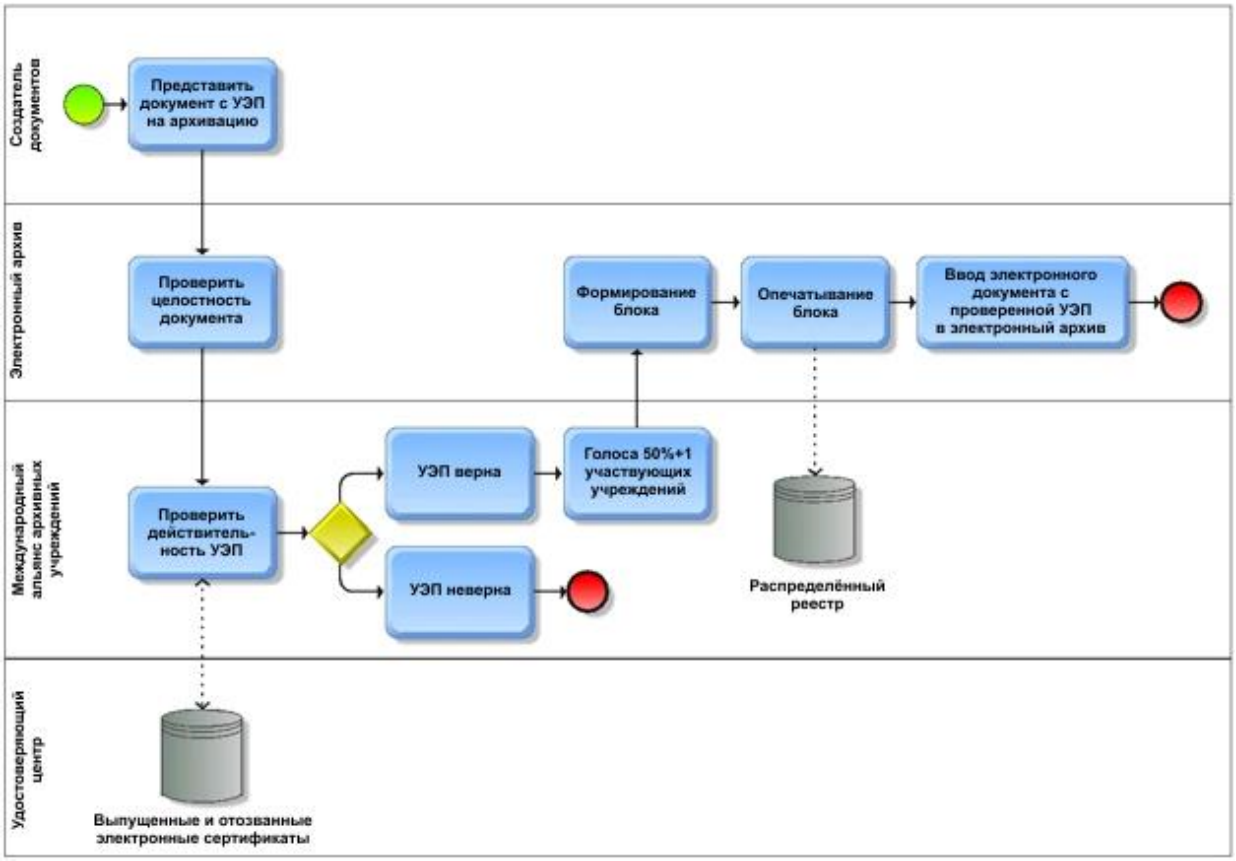


Рис. 1 – TrustChain – регистрация в блокчейне сведений о действительности усиленной электронной подписи

Используя этот подход, в будущем, когда нужно будет убедиться в аутентичности, целостности, надежности и пригодности к использованию документа (ISO 15489-1:2016) уже после истечения срока действия электронного сертификата, можно будет обратиться к информации, зарегистрированной в блокчейн-цепочке. Если документ (вместе с усиленной электронной подписью, основанной на электронном сертификате), не изменился с момента ввода в электронный архив (т.е. его хеш совпадает с тем значением, которое зарегистрировано в блокчейне); и если электронный сертификат был действителен на момент ввода (т.е. в блокчейне имеется запись об этом), можно будет сделать вывод о том, что целостность документа сохранена, и что его можно использовать, как если бы электронный сертификат всё ещё был действителен. На основании отметки времени в записи в блокчейне можно сделать вывод о том, что в этом случае ни сам документ, ни его подпись не изменились с тех пор, как они были зарегистрированы в блокчейне; и что на момент ввода, обозначенный отметкой времени, усиленная электронная подпись была действительной. Этот процесс показан на рисунке 2.

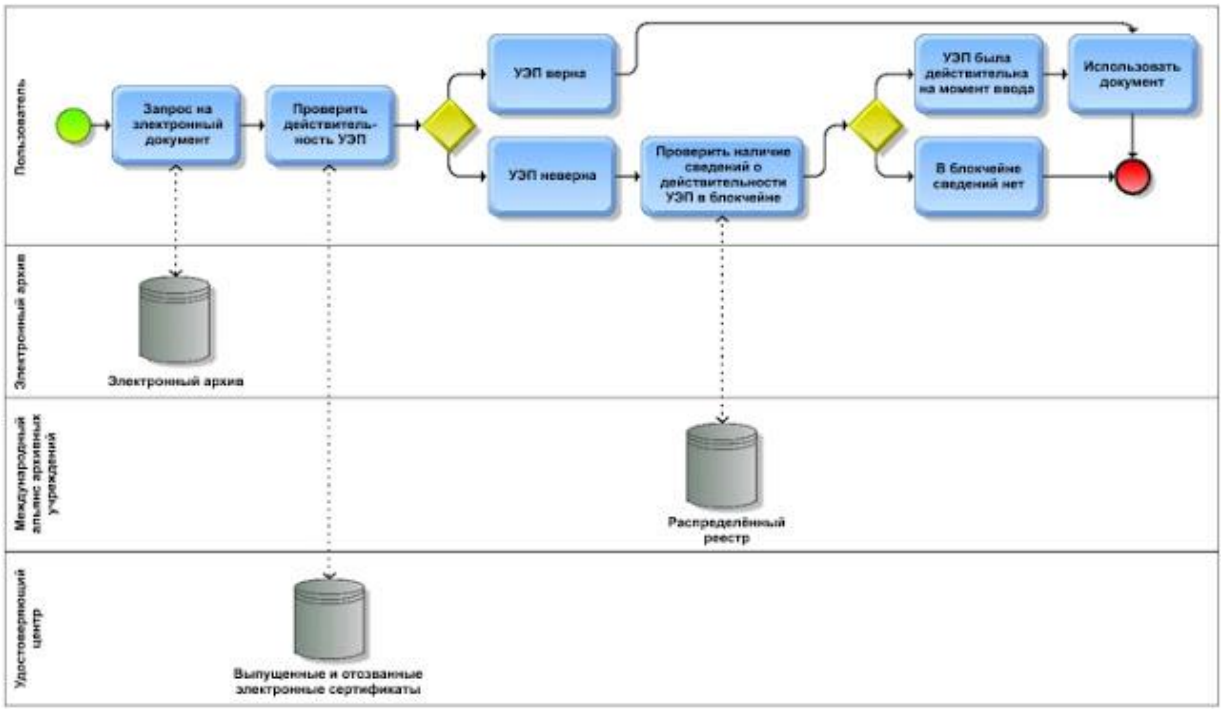


Рис. 2 – TrustChain - проверка действительности усиленной электронной подписи

Выводы

В данной статье рассмотрены проблемы обеспечения долговременной сохранности документов, подписанных усиленными электронными подписями. Вместо того, чтобы терять информацию о действительности усиленных электронных подписей из-за истечения срока действия электронных сертификатов; и вместо постоянного пере-проставления на такие документы отметок времени в моменты, когда срок действия соответствующих

электронных сертификатов вот-вот истечёт, архивы могут принять решение о внедрении решения на основе блокчейна. Предлагаемое решение TrustChain Validity Information Preservation (VIP) может быть реализовано на практике, если наберётся «критическая масса» архивных учреждений (в идеале – международный альянс), которые объединят усилия и создадут частный блокчейн (*т.е. блокчейн-решение, участниками которого является узкий круг членов такого альянса – Н.Х.*). Разумеется, архивы могут также положиться на одно из публичных блокчейн-решений, пока такая «критическая масса» не будет достигнута. Чем больше учреждений будет задействовано, тем более безопасным будет такой частный блокчейн.

Решение TrustChain может решить проблему долговременной сохранности сведений о действительности электронных сертификатов, использованных для создания усиленных электронных подписей, – но только до тех пор, пока не потребуется провести очередные действия по обеспечению электронной сохранности (*имеется в виду конверсия/миграция электронных документов, необходимая для предотвращения их морального устаревания и сохранения пригодности к использованию т.е. доступности – Н.Х.*). Например, неизбежно, что в какой-то момент времени файловый формат документа устареет и потребуется провести его преобразование в новый файловый формат. В этот момент в блокчейне должно быть зарегистрировано новое значение хеша документа, преобразованного в новый файловый формат, поскольку внесение каких-либо исправлений в уже включенные в блокчейн блоки невозможно. Тем не менее, интервалы между такими действиями по обеспечению сохранности намного длиннее (если архивный файловый формат выбран правильно), чем интервалы между переподписаниями или перепроставлением отметок времени. Таким образом, предлагаемое решение на основе блокчейна может очень хорошо дополнять обычные меры по обеспечению долговременной сохранности электронных материалов, которые одновременно будут инициировать обновление информации в блокчейне.

Дальнейшие исследования

В будущих исследованиях предполагается изучить возможности использования решения TrustChain VIP удостоверяющими центрами в процессе обеспечения сохранности цепочек сертификатов. Кроме того, планируется расширение модели с тем, чтобы включить в неё процесс сохранения сведений о действительности электронных сертификатов во время и после выполнения действий по обеспечению электронной сохранности.

Благодарности

Настоящая статья подготовлена на основе результатов исследования «Модель доверия к документам, подписанным усиленными электронными подписями, снабженными отметками времени и/или электронными печатями (модель TRUSTER)» (Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records - TRUSTER Preservation

Model), выполненного в рамках международного проекта InterPARES Trust (https://interparestrust.org)

Литература и веб-ресурсы

Blanchette, J.-F. (2006). The Digital Signature Dilemma: To Preserve or Not to Preserve. Annales des Télécommunications, 61(7-8), 908-923.

Bralić, V., Kuleš, M. and Stančić, H. (2017). A model for long-term preservation of digital signature validity: TrustChain. In: I. Atanassova, W. Zaghouani, B. Kragić, K. Aas, H. Stančić, and S. Seljan (Ed.), INFuture2017: Integrating ICT in Society, pp. 89-113, Zagreb, https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain

Croatian Encyclopedia (2017). s.n. Digitization. Miroslav Krleža Institute of Lexicography

ETSI (2016). ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation: http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

ISO 15489-1:2016, Information and documentation - Records management - Part 1: Concepts and principles, https://www.iso.org/standard/62542.html

InterPARES Trust Terminology Database, http://arstweb.clayton.edu/interlex/en/term.php?term=trustworthiness

ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (2016), http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509

RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280

Stančić, H. (2000). Digitization of documents. 2. i 3. seminar Arhivi, knjižnice, muzeji - Mogućnosti suradnje u okruženju globalne informacijske infrastrukture (pp. 64-70). Zagreb: Hrvatsko knjižničarsko društvo.

Stančić, H. et al. (2018). Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31), InterPARES Trust, https://interparestrust.org/

ПРЕЗЕНТАЦИЯ К ДОКЛАДУ ДОКТОРА ХРВОЕ СТАНЧИЧА «ВОЗМОЖНОСТИ ДЛЯ ИСПОЛЬЗОВАНИЯ БЛОКЧЕЙНА В АРХИВАХ»

Источник: YouTube https://www.youtube.com/watch?v=vq9OIqD6RMc

Презентация к докладу профессора кафедры информационно-коммуникационных наук факультета гуманитарных и социальных наук университета Загреба, Хорватия, д-ра Хрвое Станчича «Возможности для использования блокчейна в архивах» на международной конференции «От пергамена к цифре», Казань, 19 апреля 2018 года.

Возможности для использования блокчейна в архивах

Д-р Хрвое Станчич (Dr. Hrvoje Stančić), профессор кафедры информационно-коммуникационных наук факультета гуманитарных и социальных наук университета Загреба, Хорватия,
hstancic@ffzg.hr

Содержание

2

1. Введение

- Электронные документы сегодня
  - оцифрованные аналоговые документы
  - изначально-электронные документы
- Оцифровка разделяет усилия в области электронной сохранности на два направления:
  - обеспечение сохранности информационного контента
  - обеспечение сохранности физического объекта (носителя)
- Сохраняемые в электронном виде документ
  - свойства аутентичности, надёжности, целостности, пригодности к использованию (ISO 15489-1:2016)
  - доверие – точные, надёжные, аутентичные

3

1. Введение ...

- Электронная сохранность
  - упреждающий подход - действия «на опережение»
  - постоянная, непрерывная поддержка
  - зависимость от сложной экосистемы, включающей:
    - оборудование
    - программное обеспечение
    - стандарты
    - законодательно-нормативную базу

  которые непрерывно меняются, исправляются и заменяются

2. Документы, подписанные УЭП

- Усиленные электронные подписи
  - использование инфраструктуры PKI
  - опора на поставщиков услуг доверия (удостоверяющие центры), чтобы удостоверить личность подписанта
- Обеспечение идентификации личности
  - на основе электронных сертификатов
  - сертификаты обычно выпускаются на 2-5 лет
    ⇒ последствия для обеспечения долговременной сохранности

5

2. Документы, подписанные УЭП …

- Долговременная сохранность документов, подписанных УЭП
- Варианты действий электронных архивов
  1. сохранение УЭП
  2. «снятие» УЭП
  3. документирование сведений об УЭП в метаданных (подход доверенного электронного хранилища)
- Подход InterPARES Trust
  4. документирование в блокчейне сведений о действительности сертификатов

6

3. TrustChain

- Проект InterPARES Trust
  - исследование «Модель доверия к документам, подписанным усиленными электронными подписями, снабженными отметками времени и/или электронными печатями» (модель TRUSTER)
  - TrustChain – блокчейн-решение, обеспечивающие сохранение сведений о действительности сертификатов
  - группа: Хрвое Станчич (Hrvoje Stancic - руководитель), Виктория Лемьё (Victoria Lemieux), Наталья Храмцовская, Enigio Time AB, FHSS GRAs
  - идея – международный альянс архивных учреждений, выступающих в роли узлов архивного блокчейна

7

3. TrustChain ...

- В момент ввода в электронный архив
  - в блокчейне регистрируется хеш документа
  - проверяется действительность УЭП /сертификата
  - сведения о действительности регистрируются в блокчейне

впоследствии на основания отметки времени в записи в блокчейне можно сделать выводы:

- документ с момента принятия на хранение не изменился
- УЭП с момента принятия на хранение не изменилась
- электронный сертификат был действителен на момент принятия на хранение

⇒ документом можно пользоваться, как если бы сертификат всё ещё был действителен

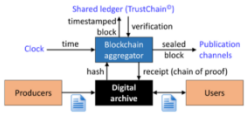
9

4. Выводы

- С чего начать? С подключения электронного архива к блокчейну через **блокчейн-агрегатор**

11

4. Выводы...



- Внедрение принципов блокчейна в ряде архивных учреждений на основе модели **TrustChain** позволит:
  - подтвердить **целостность** документа
  - что документ **существовал** к определенному момент времени (т.е. до того, как он был снабжен отметкой времени и зарегистрирован в блокчейне)
  - подтвердить **последовательность** документов
  - обеспечить/усилить **неотказуемость** документов
  - улучшить возможности для **валидации** документов с УЭП при их длительном хранении
    - сведения о действительности подписей не теряют своей силы со временем

12

4. Выводы ...

- Вместо
  - потери сведений о достоверности сертификатов ввиду истечения срока их действия, или
  - постоянное пере-проставление отметок времени

можно внедрить решение TrustChain Validity Information Preservation (VIP)

- Публичный либо частный (с регламентированным доступом) блокчейн
- «Критическая масса» (международных) учреждений
- Группа разработчиков TrustChain с удовольствием обсудит возможности для внедрения решения

13

Литература и веб-ресурсы

- Blanchette, J.-F. (2006). The Digital Signature Dilemma: To Preserve or Not to Preserve. Annales des Télécommunications, 61(7-8), 908-923.
- Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long-term preservation of digital signature validity: TrustChain. In I. Atanassova, W. Zaghouani, B. Kragić, K. Aas, H. Stančić, & S. Seljan (Ed.), INFuture2017: Integrating ICT in Society, (pp. 89-113). Zagreb. https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain
- Croatian Encyclopedia (2017). s.n. Digitisation. Miroslav Krleža Institute of Lexicography.
- ETSI (2016). ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation: http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.00_30/en_31910201v010100v.pdf
- International Organization for Standardization (2016) ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles, https://www.iso.org/standard/62542.html
- InterPARES Trust Terminology Database. http://arstweb.clayton.edu/interlex/en/term.php?term=trustworthiness
- Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (2016). http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://tools.ietf.org/html/rfc5280
- Stančić, H. (2000). Digitization of documents. 2. i 3. seminar Arhivi, knjižnice, muzeji - Mogućnosti suradnje u okruženju globalne informacijske infrastrukture (pp. 64-70). Zagreb: Hrvatsko knjižničarsko društvo.
- Stančić, H. et al. (2018). Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31), InterPARES Trust, https://interparestrust.org/

14

Спасибо!

Возможности для использования блокчейна в архивах

Д-р Хрвое Станчич (Dr. Hrvoje Stančić), профессор кафедры информационно-коммуникационных наук факультета гуманитарных и социальных наук университета Загреба, Хорватия,
hstancic@ffzg.hr

РОССИЯ СОЗДАЛА НАЦИОНАЛЬНОЕ ОБЛАЧНОЕ ХРАНИЛИЩЕ

Источник: https://portaltele.com.ua/news/technology/rossiya-sozdala-natsionalnoe-oblachnoe-hranilishhe.html

Не секрет, что когда речь заходит об использовании новейших технологий в компаниях, принадлежащих государству, хвастаться особо нечем. Практически везде можно встретить лишь сильно устаревшие компьютеры, которые связаны друг с другом при помощи ужасных сервисов, имеющих свойство постоянно выходить из строя и зависать. Впрочем, это не помешало России создать свое собственное облачное хранилище, ставшее национальным. Речь идет об аналоге Google Drive, iCloud и OneDrive.

Как удалось выяснить, Россия создала собственное «облако» для хранения различных данных, которое предназначено для Министерства обороны, однако в скором будущем его смогут использовать и другие государственные организации. Оно будет состоять из нескольких дата-центров по всей стране, объединенных друг с другом в единую сеть, подключенную к

внутренней сети ВС РФ. Отмечается, что национальное облачное хранилище не будет связано с интернетом, поэтому взломать его дистанционно не получится.

В общей сложности, на реализацию нового проекта будет потрачено порядка 390 млн рублей. Разработка сервиса уже ведется, причем она находится в заключительной стадии. К 2020 году в стране будут построены дата центры и прочая инфраструктура, необходимая для работы новой российской разработки. В первое время доступ к ней будут иметь лишь военные, однако затем ее планируется сделать общедоступной в рамках государственных компаний.

Какие именно данные будут хранить военные в рамках облачного хранилища – неизвестно. Впрочем, скорее всего, таковыми окажутся какието внутренние документы, имеющие статус важных. Нет никаких данных и о том, на какой скорости будут передаваться данные из «облака» на компьютеры. Поскольку речь идет о национальном месте хранения данных, то все данные там должны шифроваться, потому как иначе во всем этом не было бы никакого смысла.

Национальное «облако» России окажется изолировано от интернета ради того, чтобы обезопасить его от посягательств других стран. Произвести его взлом и кражу файлов можно будет исключительно в пределах глобальной локальной сети, а поскольку она окажется целиком и полностью расположена в РФ, то сделать это для США, Европы и других регионов мира окажется невозможно, потому как в случае незаконного вторжения начнется Третья мировая война.

НИДЕРЛАНДЫ ОТКАЗАЛИСЬ ОТ АНТИВИРУСОВ «КАСПЕРСКОГО» ИЗ СООБРАЖЕНИЙ БЕЗОПАСНОСТИ

Источник: http://internetua.com/niderland-otkazalis-ot-antivirusov-kasperskogo-iz-soobrajenii-bezopasnosti

Правительство Нидерландов приняло решение, что больше не будет использовать антивирусное программное обеспечение от российской компании "Лаборатория Касперского"

Министр безопасности и юстиции Нидерландов Фердинанд Грапперхаус сказал, что это является мерой предосторожности для гарантии национальной безопасности.

Компаниям, которые специализируются на вопросах защиты, также нужно завершить применение антивирусных программ "Лаборатория Касперского".

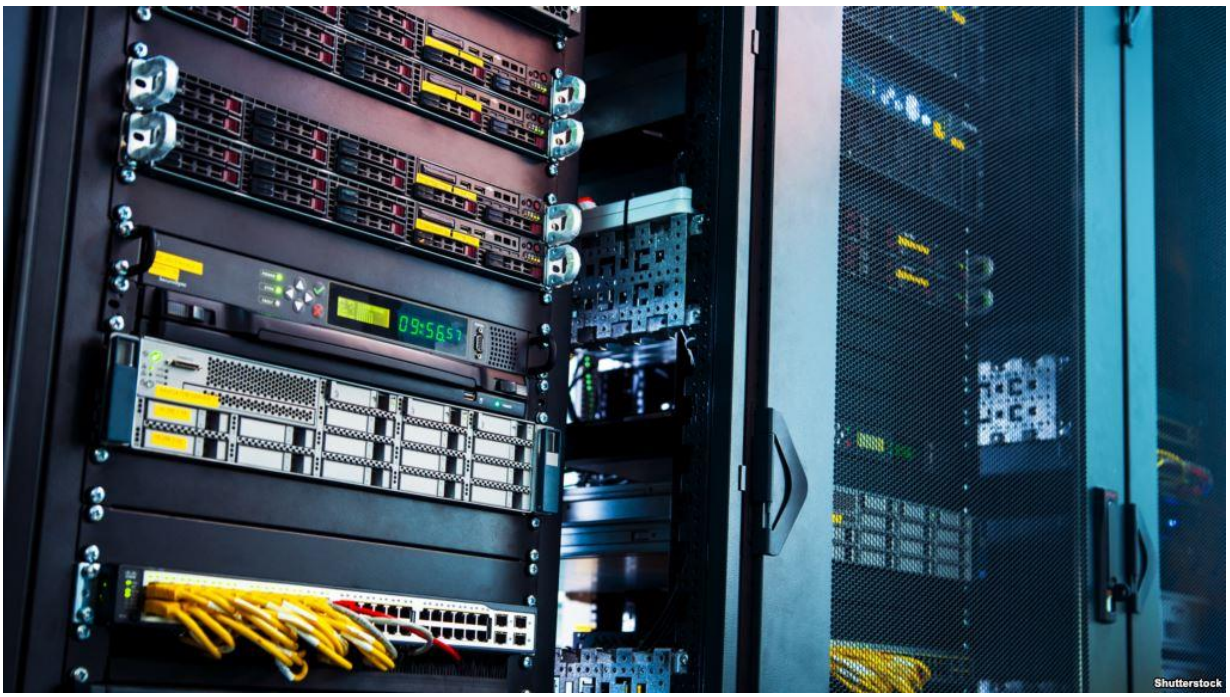
Дипломат заявил, что "Лаборатория Касперского" находится в подчинении у российского законодательства, которое обязывает компанию поддерживать российские разведывательные службы. У России имеется наступательная кибер-программа, направленная и на Нидерланды.

Он также сообщил, в Нидерландах не наблюдалось конкретных случаев злоупотребления со стороны российской компании, однако в будущем все возможно.

Мера, которую сейчас принимает правительство, относится только к антивирусу Kasperky Lab и абсолютно не касается услуг или других продуктов компании.

РІК ПІСЛЯ АТАКИ ВІРУСУ PETYA: ЩО ЗМІНИЛОСЯ В КІБЕРБЕЗПЕЦІ УКРАЇНИ

Источник:
https://www.radiosvoboda.org/a/29336511.html?utm_campaign=redtram&utm_content=421446135&utm_term=355404&utm_source=Redtram



Від початку поширення в Україні шкідливої програми Petya минув рік. Тоді вірус показав абсолютну неготовність українських державних органів та бізнесу до кібератак. Це стало причиною збитків держави у розмірі кількасот тисяч доларів та втрати інформаційних даних. Радіо Свобода розповідає, як за останній рік змінилася ситуація у кібербезпеці та як тепер відбувається захист інформації на державному рівні.

Кібератака з використанням вірусу, який спочатку був названий Petya.A (пізніше – NotPetya), відбулася наприкінці червня 2017 року. Вірус блокував комп'ютерні системи компаній, вимагаючи за розблокування 300 доларів у біткойнах.

Тоді про напад на третину банківських установ повідомив Національний банк України. Вірус також атакував компанію «Нова пошта», а також уряд, низку енергетичних компаній – у тому числі регіональних, редакції великих медіахолдингів тощо.

Служба безпеки України повідомляла, що зараження комп'ютерних систем відбувалося в декілька етапів напередодні Дня Конституції України через використання бухгалтерського програмного забезпечення.

Фахівці із кібербезпеки запевняють, що ні державні органи, ні бізнес не були готові до подібних атак, але за останній рік ситуація суттєво змінилася.

Чому відбуваються кібератаки?

Зазвичай кібератаки на бізнес чи державні органи можуть мати одну із трьох цілей. Перша – вимагання грошей та шантаж. Друга – популяризація шахрая, який здійснює напад, і остання – дестабілізація ситуації в державі.

На думку **Андрія Окаєвича**, співробітника ситуативного центру забезпечення кіберзахисту Служби безпеки України, минулорічні атаки вірусу Petya і йому подібних не мали на меті фінансового інтересу.

«Всі атаки відбувалися з метою досягнення максимальних суспільних наслідків, резонансу. Якщо була атака на казначейство – це був кінець фінансового року, якщо на «Укрзалізницю – перед вихідними, коли люди масово намагались отримати квитки», – розповідає Окаєвич.

Засновник компанії «Октава кіберзахист» **Олександр Кардаков** наголошує, що вірус Petya зупинив третину економіки України на три дні, що стало наслідком для збитків у понад 400 мільйонів доларів.

«За останній рік відбувся прорив – ухвалений закон, бізнес також почав працювати у цьому напрямку. 20% корпорацій почали серйозно займатися кібербезпекою. Ще 20-30% обговорюють створення таких систем захисту», – каже Кардаков.

Експерт вважає, що якби атаки від Petya відбувалися сьогодні, то збитки були би меншими у 5-10 разів.

Законодавче врегулювання

Суттєве зрушення, яке відбулося у сфері української кібербезпеки – законодавче врегулювання.

У травні 2018 року набув чинності закон «Про основні засади забезпечення кібербезпеки України».

Документ визначає повноваження і обов'язки державних та приватних установ, організацій та громадян у сфері кібербезпеки, та визначає базові терміни, які з’явилися в українському законодавстві вперше. Наприклад, кіберзагроза, кібершпигунство чи кіберзлочинність.

Закон передбачає створення Національної телекомунікаційної мережі та Державного центру кіберзахисту.

Андрій Окаєвич зазначає, що зараз триває робота над підзаконними актами, які, наприклад, регулюватимуть обов’язкові заходи у сфері кібербезпеки для державних органів та органів критичної інфраструктури (наприклад, енергетичні компанії).

Сьогодні закон передбачає кіберзахист цих компаній на власний розсуд.

«Протягом останнього року державні органи працювали над власними помилками та аналізували досвід інших країн. Активно розвивається приватне і державне партнерство. З’явилися платформи з обміну інформацією про кіберзагрози в реальному режимі часу», – розповідає Окаєвич.

Реакція бізнесу та поради громадянам

Після атаки вірусу Petya бізнес зрозумів, що треба вкладати кошти не лише у фізичну охорону об’єкту, оскільки кібернапади мають більший потенціал збитків.

«В Україні трапляються не тільки кримінальні злочини. Кібератаки підтримує держава-агресор і вони полягають у використанні новітніх технологій, які не були відомі раніше. Саме це нас стимулює приділяти більше уваги кібербезпеці», – каже Андрій Окаєвич.

За його словами, ситуативний центр забезпечення кіберзахисту СБУ сьогодні готовий протидіяти кібератакам: там працює спеціальна лабораторія для аналізів загроз та спеціалізований персонал.

Станіслав Самойлов, начальник першого відділу Управління інформаційних технологій та програмування Департаменту кіберполіції Національної поліції України, каже, що кількість злочинів у сфері кібербезпеки за останній рік збільшилась утричі.

Представник кіберполіції також зазначає, що кількість злочинів у сфері кібербезпеки за останній рік збільшилась утричі.

Для пересічних громадян Самойлов радить бути обережними з програмним забезпеченням.

«Якщо виникли підозри, що з вашими даними відбувається щось незаконне, перш за все, варто просто вимкнути мережу інтернет. Щоб не втратити дані, потрібно завжди робити копії і зберігати їх на носіях, що не під’єднані до мережі. Інформацію краще зберігати у зашифрованому вигляді у хмарному сховищі, тоді втрачені дані можна відновити», – каже Самойлов.

Кібербезпека в державних компаніях

Микола Метьолкін, менеджер з корпоративних продажів групи компаній БАКОТЕК, вважає, що з технічної точки зору, в установ мають бути рішення не лише для захисту, але і для виявлення та реагування на атаки.

«Сьогодні лише архітектура адаптивної безпеки може найбільш ефективно протидіяти цілеспрямованим атакам. На жаль, багато державних

закупівель у сфері рішень безпеки проводяться ситуативно. Будується надто розрізнена інфраструктура і ускладнюється управління всіма рішеннями в IT-інфраструктурі установи. Це значно підвищує сукупну вартість володіння і супровідної підтримки рішень і призводить до неефективного використання державних коштів», – каже Метьолкін.

Експерт зазначає, що серед ключових моментів інформаційної безпеки є не лише технології, а й фахівці, які з ними працюють.

У найближчі роки нестача кваліфікованих фахівців зі сфери інформаційної безпеки в державних установах буде відчуватися особливо гостро. Це стосується не лише України, а і більшості країн Європи та США.

Метьолкін вважає, що закон «Про основні засади забезпечення кібербезпеки України» суттєво поліпшить ситуацію із кібербезпекою.

«Документом визначені не лише правові та організаційні засади у сфері кібербезпеки, а й закріплена відповідальність керівників підприємств, що входять до переліку об'єктів критичної інфраструктури. Вони мають слідкувати за забезпеченням безпеки комунікаційних і технологічних систем, захистом технологічної інформації, проведенням незалежних аудитів інформаційної безпеки на підприємствах та невідкладним інформування урядової команди реагування про інциденти кібербезпеки», – розповідає Метьолкін.

Експерти наголошують, що після нападу Petya захист даних в Україні став не пасивним, а активним – компанії почали працювати на випередження.

НОВАЯ КИБЕРАТАКА НА УКРАИНУ: ЧТО ТАКОЕ ВИРУС VPNFILTER И КАК С НИМ БОРОТЬСЯ

Источник:
https://ru.espreso.tv/article/2018/05/29/novaya_kyberataka_na_ukraynu_chto_takoe_vyrus_vpnfilter_y_kak_s_nym_borotsya

По данным компании Cisco, в мире появился новый вирус VPNFilter. На этот раз основной целью кибератаки стали роутеры украинских пользователей

23 мая американский разработчик сетевого оборудования компания Cisco предупредила о более чем 500 тысячах зараженных роутеров и маршрутизаторов. Как сообщает компания, вирус VPNFilter был обнаружен в 54 странах, однако основная цель хакеров – Украина. К таким выводам пришли специалисты Cisco, после “всплеска” кибератак в Украине 8 мая. Cisco имеет также свою киберразведку – Cisco Talos, где уверены, что за кибератакой стоит российское правительство.

После публикации информации, правительство США сообщило, что оно будет бороться с хакерами, которые захватили контроль над сотней тысяч зараженных маршрутизаторов и устройства хранения. Для этого Федеральный

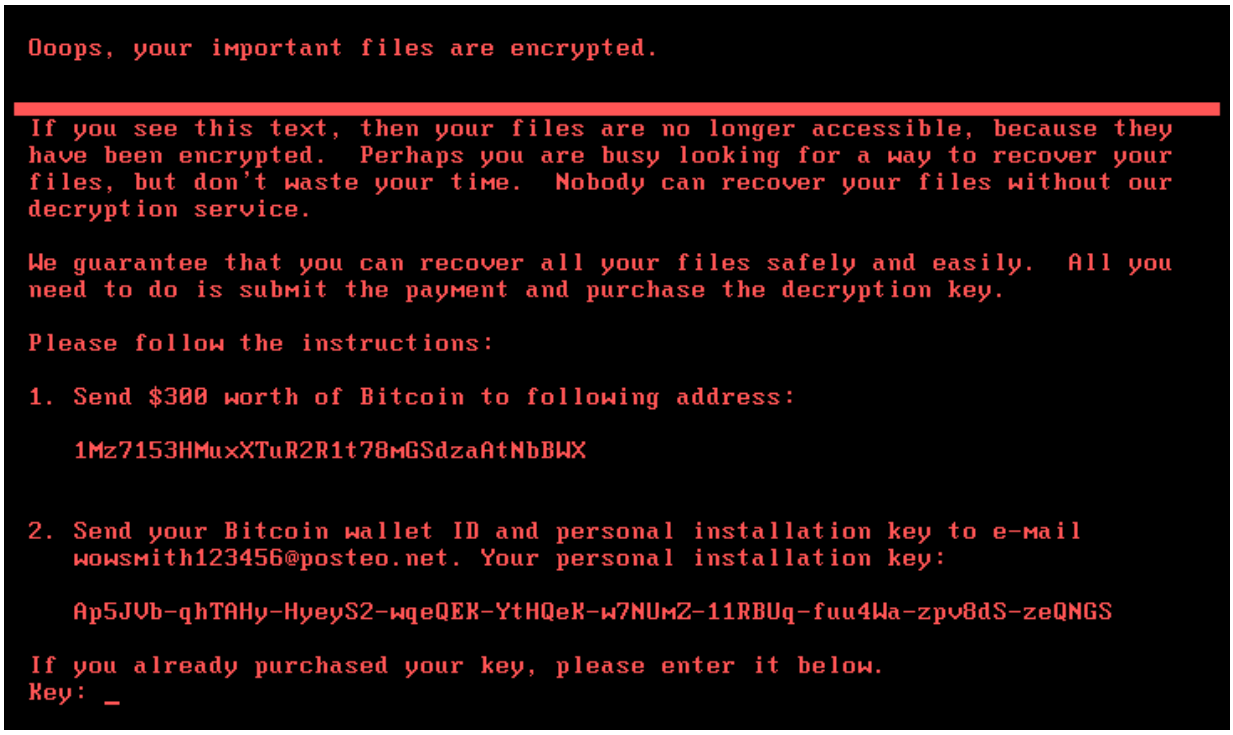
суд в Пенсильвании дал разрешение ФБР взломать домен в Интернете, через который, по подозрению властей США, хакеры управляют зараженными устройствами.

Если домен действительно является инструментом хакеров по контролю над устройствами жертв кибератаки, то после взлома удастся отследить все зараженные устройства.

Пока что вирус не находится в активной стадии, чтобы его заметить. Скорее всего, его активируют к определенной значимой дате для страны. Киберполиция ранее считала, что такой датой станет суббота 26 мая, когда начался футбольный финал Лиги чемпионов. Однако расслабляться не стоит – впереди ещё несколько важных для страны дат.

Почему такое название: “VPNFilter”? Дело в том, что вирусу нужно замаскировать свои файлы. VPN сервисы – одни из самых распространенных программ среди пользователей. Поэтому папка на устройстве с подобным названием не у всех вызовет подозрение. Пользователь просто подумает, что это очередная системная папка и не станет в нее заглядывать.

Будет как с вирусом Petya.A?



Летом 2017 года по всему миру началась массовая атака вируса-вымогателя Petya.A, которій шифровал данные компьютеров своих жертв

Нет, на этот раз вирус под названием VPNFilter заражает роутеры и маршрутизаторы, через которые получает доступ ко всей подключенной к каналу технике. Это кибератака Интернета вещей, то есть всех устройств, которые подключаются к сети и взаимодействуют друг с другом без вмешательства человека.

Если у вас есть умный холодильник, который подключен к зараженному роутеру, то вполне возможно, что хакеры смогут его отключить или изменить его настройки. Последствия от этого не самые приятные, но гораздо страшнее, если хакеры получат доступ к объектам критической инфраструктуры и жизненно важным объектам, которые давно автоматизированы. Например, при контроле энергетического сектора, хакеры смогут отключить свет во всем городе.

Как он работает?

Вирус VPNFilter умеет самоуничтожаться, тем самым выводя из строя контролируемую технику. Помимо этого, вирус может долго незаметно присутствовать на устройстве для сбора информации. Вирус состоит из трех этапов развития. Первый этап VPNFilter обеспечивает стабильность программы. То есть вирус способен “выжить” после перезагрузки в отличие от подобных вирусов для Интернета вещей.

На втором этапе вирус собирает метаданные, выполняет команды, фильтрует данные. На этой стадии хакеры через программу могут управлять устройствами. Некоторые версии вируса VPNFilter умеют самоуничтожаться, переписывая прошивку устройства. После перезагрузки “перепрошитая” вирусом техника выходит из строя.

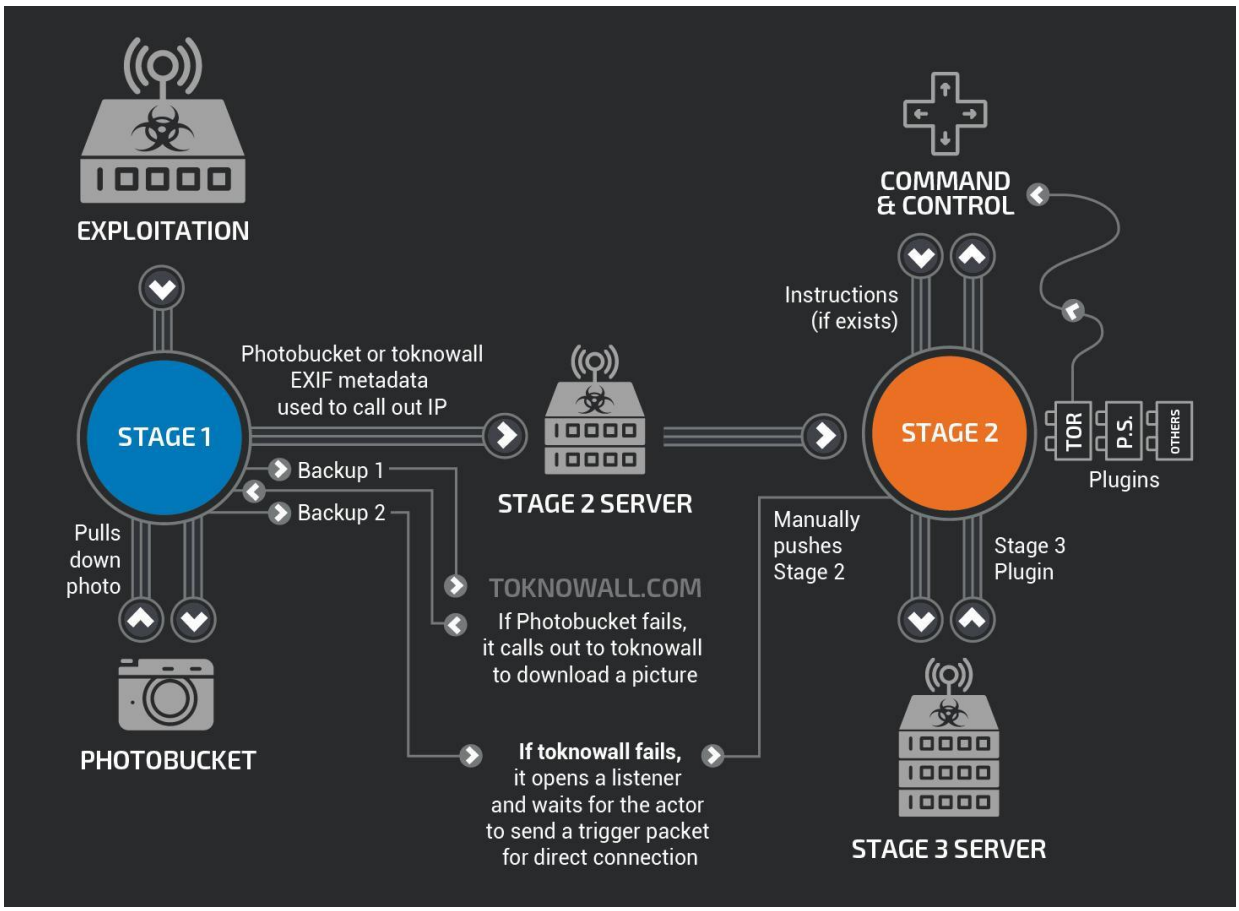
Третий этап вредоносного ПО действует как дополнение для второго этапа. Специалисты Cisco Talos пока что выявили два модуля к вирусу: программа начинает работать как “сниффер” – перехватчик всего сетевого трафика (от паролей до данных SCADA Modbus, который используется на автоматических устройствах). Или же подключается к серверу злоумышленников через службу анонимного браузера Tor.

По мнению специалистов, это вредоносное ПО используется для создания расширенной, труднодоступной инфраструктуры по контролю над важными для жизни государства секторами.

Кто находится под угрозой?

- На данный момент зафиксировано заражение этих моделей устройств:
- Linksys Devices: E1200, E2500, WRVS4400N;
- Mikrotik RouterOS (Bci вepcii що нижче 6.42.1)
- Netgear Devices: DGN2200, R6400, R7000, R8000, WNR1000, WNR2000;
- QNAP Devices: TS251, TS439 Pro, Other QNAP NAS devices running QTS software;
- TP-Link Devices R600VPN.

Однако, даже если марки вашего устройства в списке нет, если оно не было защищено надежным паролем, то риск заражения остается очень высоким.



В блоге Talos Cisco можно ознакомиться с детально технической характеристикой вируса

Как защититься?

Защита от этого вируса чрезвычайно сложна из-за природы подвергаемых атаке устройств. Большинство из них подключены непосредственно к Интернету, без каких-либо устройств безопасности или антивирусов.

Если вы подозреваете, что ваше устройство было заражено, то обнулите его настройки до заводских. Для этого на корпусе самого устройства есть кнопка “reset”. После перезагрузки необходимо настроить роутер, а для безопасности поставить на него пароль. По совету Киберполиции Украины, также поможет установка новой версии ПО на роутер, так как некоторые производителей оборудования уже выпустили ПО, которое борется с вирусом.

У роутера есть свое меню. Чтобы зайти в меню подключенного роутера в адресной строке браузера следует набрать 192.168.0.1. или 192.168.1.1. (в зависимости от модели роутера).

Если роутер запросит пароль после сброса настроек, то его можно также увидеть на нижней крышке корпуса устройства. После того, как вы зашли в меню, обязательно поменяйте стандартній заводской пароль и имя пользователя.

Можно также разрешить доступ в меню роутера только для одного устройства с определенным IP. При любом вопросе связывайтесь со службой

поддержки компании, чье оборудование вы используете, а также с провайдером, который предоставляет интернет-услуги.

Кто атакует?

Такой логотип для своей команды использовали хакеры Fancy Bear (они же APT28 и Sofacy) для сайта, посвященного взлому Антидоппингового олимпийского комитета

Компания Cisco и правительство США связывают кибератаку с хакерской группировкой Sofacy. Хакеры также известны и под другими именами: "Fancy Bears", "APT28", "Tsar Team". Название команды разнятся из-за разных инструментов, которые хакеры применяют во время атак. Sofacy работают с 2008 года.

Хакеры из группы Sofacy в основном атакуют сектора обороны, энергии, правительства, средства массовой информации США и европейских стран. Список атак команды обычно совпадает со списком интересов правительства Российской Федерации, из-за чего был сделан вывод о принадлежности хакеров к Главному разведывательному управлению России (ГРУ).

У хакеров есть собственные разработки (XAgent, X-Tunnel, WinIDS, Foozer и DownRange) которые поражают операционную систему Windows и некоторые мобильные системы. Sofacy известна тем, что регистрирует домены, которые очень похожи на домены существующих организаций, чтобы выманить пароли и логины (фишинг). Именно это произошло в 2016 году, когда один из членов Демократической партии США попытался зайти на электронную почту. Вместо этого пользователь заполнил форму сайта-фальшивки. В результате ошибки, хакеры получили доступ к почтовому серверу партии. Sofacy также связывают с атаками на немецкий бундестаг и телевизионную станцию TV5 Monde Франции в 2015 году.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ

Источник: КиберЛенинка: https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-informatsionnyh-resursov-predpriyatiya

В статье рассмотрено обеспечение безопасности информационных ресурсов предприятия. Для обеспечения высокого уровня информационной защиты требуется комплекс мер, включающий в себя функции программного обеспечения и реализация мероприятий по защите, не противоречащих законодательству. Сделан вывод: что согласно статистическим данным более 80% компаний и агентств несут финансовые убытки из-за нарушения безопасности данных. Только объединив усилия разных специалистов, можно создать эффективную систему защиты.

Введение. Информационная безопасность является одной из важных проблем, с которой столкнулось современное общество. Такая проблема возникла в результате роста ценности информации.

Понятие «информационная безопасность» в Законе РФ «Об участии в международном информационном обмене» определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие, а также характеризуется состоя-нием защищенности национальных интересов, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Актуальность. В настоящее время изучение существующих информационных систем и областей применения данных технологий, а также разработка новых методов по использованию информационных систем и технологий являются показателями актуальности данной темы[1 – 3].

Федеральный закон от 27 июля 2006 года № 149 – ФЗ «Об информации, информационных технологиях и защите информации», вступивший в силу со всеми изменениями и дополнениями 10 января 2016 года, определяет следующие понятия, регулирующие данную сферу человеческой деятельности.

Согласно данному федеральному закону под информацией понимаются любые сведения независимо от формы их представления. То есть информация может быть представлена в нескольких видах, таких как устная, письменная, звуковая, зрительная, объемно-пространственная и другие. Исходя из этого, можно сделать вывод, что все, что нас окружает, несет определенную информацию.

Процессы, методы сбора, обработки, хранения и предоставления информации, а также способы осуществления таких процессов называются информационными технологиями [4].

Развивались информационные технологии в несколько этапов:

Первый этап – использование ручных информационных технологий и основывались они на следующих инструментах: перо, чернильница и книга.

Обмен всей информацией осуществлялся через отсылку писем. Данный этап продлился до половины XIX века.

Второй этап – использование механических технологий и основывались они на следующих инструментах: пишущая машинка, телефон, диктофон и почта. Данный этап продлился с конца XIX века по 40-е годы XX века.

Третий этап – использование электрической технологии, косновным инструментам которой относят большие ЭВМ и соответствующее программное обеспечение, электронные пишущие машинки, ксероксы, портативные диктофоны. Данный этап датируется 40 – 60 годами XX века.

Четвертый этап – использование электронной технологии как автоматизированного процесса управления деятельностью. Теперь передача данных не является основной целью развития электронных технологий. Теперь было важно раскрыть суть содержания информации. Для этого использовались следующие инструменты: ЭВМ, автоматизированные системы управления, информационно-поисковые системы. Данный этап определен в 70-х годах XX века.

Пятый этап – развитие компьютерной технологии, главным инструментом которой стал персональный компьютер. Данный этап датируется с 80-х годов XX века по нынешний день и характеризуется массовым использованием локальных и глобальных компьютерных сетей.

Информационные технологии играют важнейшую роль в обеспечении взаимодействия между людьми, а также в распространении массовой информации. Они быстро ассимилируются культурой нашего общества, так как не только создают большие удобства, но и решают многие производственные, социальные, бытовые и культурные проблемы, вызываемые процессами в мировом сообществе, расширением международных связей и другими процессами в обществе [5].

Современные информационные технологии шагнули далеко вперед и будут развиваться еще больше. Сейчас информационная система представляет собой совокупность информации, содержащейся в базах данных, и технологии, обеспечивающих ее обработку. Если заглянуть в понятие «информационная система» более детально, то можно сделать вывод о том, что стабильное функционирование системы базируется как минимум на шести обеспечивающих ее подсистемах [6].

К таким подсистемам, согласно рисунку 1 выше относят: программное, техническое, правовое, информационное и эргономическое обеспечения.

Для отдельной организации под информационной безопасностью понимается стабильное состояние информационной среды, которая не подвергается несанкционированному взлому извне. Другими словами, информационная безопасность, в частности, в сфере туризма и гостеприимства понимается как защищенность информации и поддерживающей ее инфраструктуры от воздействия естественного и искусственного характера, которые могу нанести ущерб владельцам или потребителям данной информации.

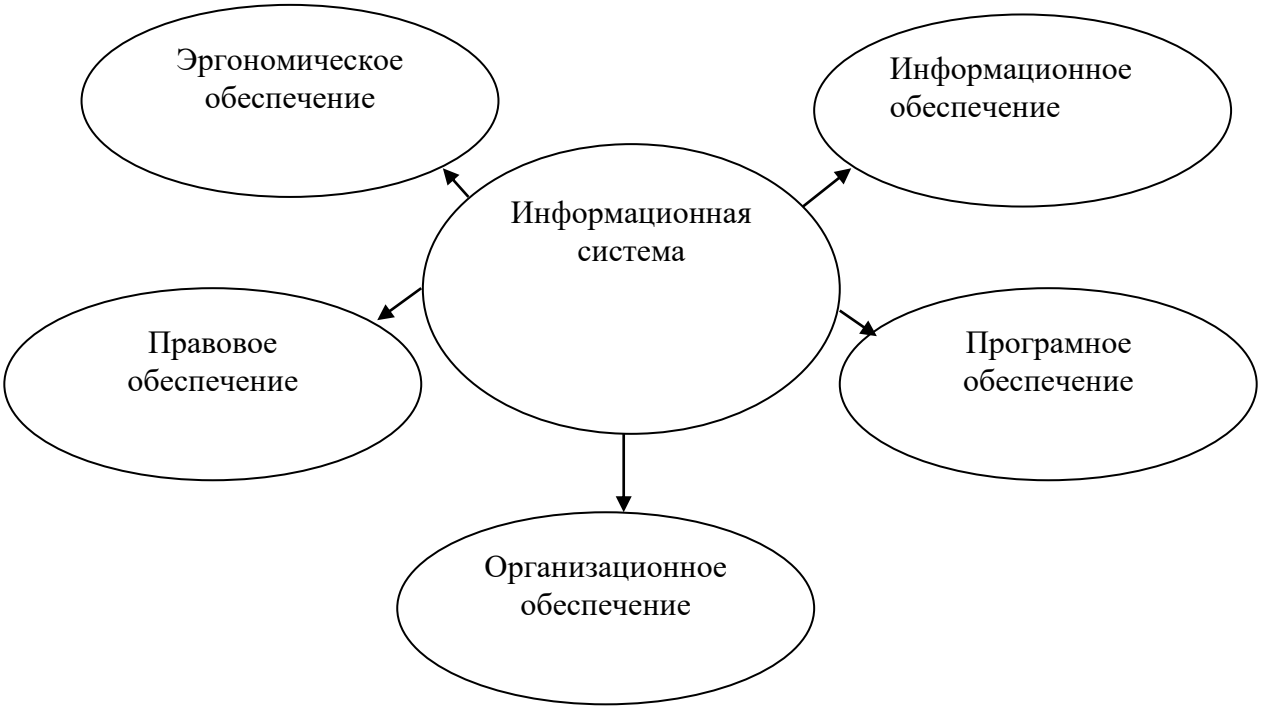


Рис.1. Структура информационной системы

Рис. 2. Признаки корпоративных данных компании

Под указанными в рисунке 2 признаками понимаются:

• под конфиденциальностью понимается обеспечение ограниченного доступа к информации, то есть доступ, имеют лишь зарегистрированные пользователи;

• под целостностью, понимается полнота и достоверность информации;

• под доступностью понимается обеспечение доступа к информации по мере необходимости.

Под защитой информации понимается мероприятия по предотвращению случайного или преднамеренного воздействия, чаще негативного, на информационную среду, а также утечки защищаемой информации.

Действия по защите информационных ресурсов в организации осуществляется силами самой организации, путем формирования

соответствующих подразделений, а также специальными государственными органами, такими как Федеральная служба безопасности, Министерство внутренних дел РФ, Совет безопасности РФ, а также Служба по контролю в сфере связи, информационных технологий и массовых коммуникации [7].

Вывод. На каждом предприятий, где имеется сфера конфиденциальных данных, в обязательном порядке принимается стандарт информационной безопасности, а также определяется категория сотрудников, имеющая постоянный доступ к данной информации, в связи с чем они подписывают внутренний документ о неразглашении.

ЛИТЕРАТУРА:

1. Алексеенко В. Н., Сокольский Б. Е. Система защиты коммерческих объектов. Технические средства защиты. // Практическое пособие для предпринимателей. – М., 2002.

2. Батурин Ю. М., Жоздишеаский А. М. Компьютерная преступность и безопасность. – М., 2002.

3. Борисов И. Н. Анализ услуг в области безопасности // Безопасность предпринимательства и личности, 2005, № 1, январь.

4. Герасименко В. А. Основы зашиты коммерческой информации и интеллектуальной собственности в предпринимательской деятельности. – М., 2001.

5. Мезеркин Д. Аналитическая работа службы безопасности предприятия. //Частный сыск, охрана, безопасность, 2003, № 1.

6. Тюменев А. В. Обеспечение безопасности и система правового регулирования в сфере физической культуры и спорта при проведении спортивно – массовых мероприятий / Тюменев А. В., Панов Н. Н. // В сборнике: ФИТНЕС-АЭРОБИКА-2016 материалы Всероссийской научной интернет-конференции. 2016. С. 8 – 14.

7. Тюменев А. В. Модели оценки безопасности обеспечения информационных ресурсов в вузе / Тюменев А. В., Панов Н. Н. // В сборнике: Современные тенденции развития науки и образования: теория и практика Материалы 1 Международнйо научно-практической конференции научно-педагогических работников и молодых ученых. Под ред. Г. С. Жуковой; Центр математического образования Московского политехнического университета. 2017. С. 303 – 312.

УПРАВЛЕНИЕ МЕТАДАННЫМИ ДОКУМЕНТОВ ПОСТОЯННОГО СРОКА ХРАНЕНИЯ: КАК БЫТЬ, ЕСЛИ МЕТАДАННЫЕ, ТРЕБУЕМЫЕ ДЛЯ ПЕРЕДАЧИ ДОКУМЕНТОВ НА АРХИВНОЕ ХРАНЕНИЯ, ХРАНЯТСЯ ОТДЕЛЬНО ОТ САМИХ ДОКУМЕНТОВ?

Источник: блог «Records Express» на сайте NARA https://records-express.blogs.archives.gov/2018/05/31/managing-metadata-for-permanent-records-what-if-the-metadata-required-for-transferring-permanent-records-are-stored-separately-from-the-records-themselves/

Продолжая тему о требованиях к метаданным документов постоянного срока хранения на общих дисках (Metadata Requirements for Permanent Records on Shared Drives, 4 декабря 2017 года, см. https://records-express.blogs.archives.gov/2017/12/04/metadata-requirements-for-permanent-records-on-shared-drives/), мы обсудим, как управлять метаданными документов постоянного срока хранения, если они хранятся отдельно от документов.

Для необходимых метаданных, как указано в бюллетене NARA 2015-04 «Руководство по метаданным, требуемым при передаче на архивное хранение электронных документов постоянного срока хранения» (NARA Bulletin 2015-04: Metadata Guidance for the Transfer of Permanent Electronic Records, http://www.archives.gov/records-mgmt/bulletins/2015/2015-04.html, *о нём см. также пост* https://rusrim.blogspot.com/2015/09/blog-post_21.html), должны быть установлены те же сроки хранении и действия по их истечении, что и для документов, которые они описывают – независимо от того, хранятся ли они в отдельной системе, в приложении для управления документами или же в системе управления досье/заказами/запросами на обслуживание (case management system). Метаданные должны захватываться и затем управляться на протяжении всего жизненного цикла документов, а также сопровождать документы при передаче их на архивное хранение.

Некоторые приложения и файловые форматы хранят метаданные в файле структурированным способом, или же поддерживают использование стандартизованных схем, таких, как поля метаданных Adobe XMP или XML в формате JPEG 2000. В противном случае большинство метаданных будет находиться во внешних базах данных, системах или реестрах. Обычно для установления связи хранимых во внешней системе метаданных с файлами графических образов в каталоге используются уникальные идентификаторы или имена файлов графических образов.

Хранение метаданных в отдельной системе, такой, как база данных, обеспечивает большую гибкость при управлении, использовании и преобразовании. В числе других преимуществ можно назвать поддержку многопользовательского доступа к данным, продвинутую индексацию,

сортировку, фильтрацию и обработку поисковых запросов. Поддерживаемые во внешних системах метаданные могут содержать иерархическую описательную и структурную информацию о многостраничных или сложных объектах и облегчать импорт, экспорт и сбор данных во внешние системы или иные форматы, такие как XML.

Бет Крон

РОСАРХИВ ВЫЛОЖИЛ ПРОЕКТ «ТИПОВЫХ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМАМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И СИСТЕМАМ ХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В АРХИВАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ»

Источник: http://archives.ru/sites/default/files/2018-06-14-project-tft.doc
Автор: Наташа Храмцовская

14 июня 2018 г. на официальном сайте Федерального архивного агентства (Росархива) в разделе «Проекты документов» размещен проект «Типовых функциональных требований к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов» объёмом 37 страниц.

Театр начинается с вешалки, а любой разработанный Росархивом документ – с очередного «подхода» к терминологии. Некоторые из определений вполне могли бы претендовать на приз за невнятность и некорректность (их многократно ругали на протяжении последнего десятилетия, но Росахиву не откажешь в умении не прислушиваться к критике):

Документ – ***официальный*** документ, созданный государственным органом, органом местного самоуправления, ***юридическим или физическим лицом,*** оформленный в установленном порядке ***и включенный в документооборот ГО***;

Аутентичность (электронного документа) – свойство электронного документа, гарантирующее, что электронный документ идентичен ***заявленному***;

Схема классификации – иерархически организованная совокупность оснований классификации, состоящая из разделов и подразделов в соответствии с которыми организуется систематизация и организация хранения документов в СЭД /СХЭД ГО;

Обращает на себя внимание определение контейнера электронного документа, которое жёстко предписывает определенные технические решения:

Контейнер электронного документа – zip-архив, включающий контент и метаданные электронного документа, файлы электронных подписей и визуализированную копию текстового электронного документа в формате PDF/A;

Важным моментом является очень широкое определение «системы электронного документооборота», под которое, с моей точки зрения, подпадают практически все информационные системы, как специализированные системы для управления документами, так и деловые:

Система электронного документооборота (СЭД) – автоматизированная информационная система, обеспечивающая создание электронных документов, включение документов с систему и управление ими в течение времени;

Мои основные претензии к документу – те же, что и в предыдущих случаях:

- У разработчиков нет четкого видения роли данного документа – какую отдачу он должен дать, равно как и понимания возможности реализации на практики такого рода требований и связанных с этим временных и финансовых затрат. Говоря попросту, никто сейчас не выделит миллиарды рублей на замену СЭД в масштабах государства, а разработчикам СЭД на сколько-нибудь серьёзные доработки понадобится не менее пары лет (и опять же деньги!);
- Отсутствуют высокоуровневые требования – что именно хорошая СЭД должна обеспечивать. Не проводится четкой грани между документными и деловыми информационными системами. Авторы сразу углубляются в относительно мелкие технологические и функциональные детали, которые к тому же быстро устаревают по мере развития технологий; В целом в требованиях старательно отражена технология отечественных СЭД примерно десятилетней давности т.е. того поколения решении, которое в ближайшие годы будет выводиться из эксплуатации.
- Как обычно, Росархив не в курсе существования во Вселенной чего-либо кроме традиционных организационно-распорядительных документов, что отразилось и на составе требований.

Сами требования в целом производят не такое уж плохое впечатление, там есть много разумного. Видно, что авторы документа серьёзно изучали имеющуюся на русском языке литературу. Однако требования плохо структурированы, и, на мой взгляд, разработчикам программного обеспечения работать с ними будет очень неудобно.

Подводя итог, скажу, что, с моей точки зрения, серьёзных перспектив практического применения у этого документа нет никаких, однако он довольно любопытен как отражение хода развития отечественной документационной науки.

Могу предположить, что наши ведомства или вообще «не заметят» этот документ (как это было с предыдущими требованиями Минкомсвязи), или

будут настаивать на том, что у них нет систем типа СЭД/СХЭД, о которых в требованиях идёт речь.

ЧЕХИЯ: КРАТКИЙ ОТЧЕТ О МЕЖДУНАРОДНОМ СЕМИНАРЕ «АРХИВЫ В ЭЛЕКТРОННУЮ ЭПОХУ» AIDA-2018

Источник: блог «Digital Preservation CZ» http://www.digitalpreservation.cz/2018/05/archives-in-digital-age-aida-2018-v-na.html
Автор: Наташа Храмцовская

10 и 11 мая 2018 года на площадке Национальных Архивов республики Чехия прошёл международный семинар из серии «Архивы в электронную эпоху» (Archives in Digital Age, AIDA-2018). Это было уже третье ежегодное мероприятие, и на этот раз основное внимание было уделено вопросам аудита и сертификации электронных хранилищ. Одной из позитивных сторон семинара стало объединение усилий архивного и библиотечного сообществ вокруг темы электронных хранилищ. Хотя архивисты определенно были представлены лучше, но и у библиотечного сообщества были свои представители, по крайней мере, из Национальной библиотеки и Библиотеки Моравии.

Мой комментарий: *официальная тема семинара звучала так: «Само-аудит и сертификация электронных хранилищ в центрально-европейской перспективе» (Self-Audit and Certification of Digital Archives in Central European Perspectives). Программа мероприятия выложена по адресу* http://cesarch.cz/blog/2018/05/22/mezinarodni-workshop-aida-2018/

Несомненно, наиболее полезным был, конечно же, доклад Христиана Кейтеля (Christian Keitel) из Архивов земли Баден-Вюртемберг (Германия), который является членом немецкой ассоциации Nestor (*сокращение от Network of Expertise in Long-Term Storage of Digital Resources - Сеть обмена опытом в области долговременного хранения электронных ресурсов – Н.Х.*). Эта ассоциация разработала стандарт DIN 31644, который используется в Германии для сертификации доверенных электронных хранилищ (будь то хранилища библиотек, архивов или других учреждений, занимающихся сохранением культурно-исторической памяти). Рассказ Кейтеля о его опыте разработки этого стандарта и проведения аудитов на соответствие его требованиям, конечно же, оказался весьма информативным и ценным. Хотя стандарт DIN 31644 отражает условия немецкой среды, однако благодаря крепким связям с коллегами из Федерального архива Германии намечается возможность сотрудничества и переноса этого стандарта в чешскую среду (по крайней мере, архивную).

Мой комментарий: *Речь идёт о немецком стандарте DIN 31644:2012 «Информация и документация – Критерии для доверенного электронного архива» (Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive, английское название Information and documentation - Criteria for trustworthy digital archives), о нём см.* http://rusrim.blogspot.com/2010/08/blog-post_6895.html. *Содержание стандарта (на немецком языке) выложено здесь:* https://www.din.de/en/getting-involved/standards-committees/nid/standards/wdc-beuth:din21:147058907/toc-1854419/download

Национальные Архивы Чехии сейчас планируют перевести «Разъяснения в отношении «печати качества» ассоциации Nestor для доверенных электронных архивов» (Explanatory notes on the Nestor Seal for Trustworthy Digital Archives – *в сети выложены версия 2 на немецком языке, см.* https://d-nb.info/1118881362/34 , *и версия 1 на английском языке, см*. https://d-nb.info/1047613859/34 – *Н.Х.*) Это может быть очень полезным, так как DIN 31644 не столь сложен, как международный стандарт ISO 16363:2012 «Системы передачи данных и информации о космическом пространстве – Аудит и сертификация доверенных электронных хранилищ» (Space data and information transfer systems - Audit and certification of trustworthy digital repositories, см. https://www.iso.org/standard/56510.html и https://www.iso.org/obp/ui/#iso:std:iso:16363:ed-1:v1:en), но при этом обеспечивает необходимую сертификацию доверенного электронного хранилища. В чешских условиях стандарт DIN 31644 теоретически может стать заменой для аудита или даже полноценной сертификации на соответствие требованиям ISO 16363.

Мой комментарий: *Стандарт ISO 16363 – это, по сути дела, снабжённый обложкой ИСО документ CCSDS 652.0-M-1 с тем же названием, подготовленный Консультативным комитетом по системам хранения данных космических исследований (Consultative Committee for Space Data Systems, CCSDS) и доступный свободно по адресу* http://public.ccsds.org/publications/archive/652x0m1.pdf.

Зденек Вашек (Zdeněk Vašek) из Архивов Карлова университета в своем выступлении подытожил пользу от сертификации в условиях Чехии – любопытно, что два из трех хранилищ, получивших сертификат «электронной печати качества» (Data Seal of Approval, DSA), не стали его обновлять по истечения срока действия. Вероятно, это связано с тем, что на первоначальный проект подготовки необходимых документов и проведения сертификации средства были выделены, а на повторную сертификацию денег найти не удалось.

В докладе также был дан интересный комментарий по поводу ситуации в Чехии – о сертификации много говорят, стандарт DSA очень популярен в стране (есть два перевода, выпущенные в 2013 и 2016 годах), и все знают о пользе от сертификации – но практически никто не занимается сертификацией собственного электронного хранилища. Автор связывает такое положение дел с затратами времени и труда на проведение сертификации, с разобщённостью

профессионального сообщества и с тем фактом, что в Чехии нет согласия относительно единого стандарта.

В связи с этим важно, какую позицию займёт Национальная библиотека Чехии, единственная из библиотек республики, у которой есть электронное хранилище для обеспечения долговременной сохранности. Уже несколько лет идут разговоры о том, что Национальная библиотека планирует провести сертификации своего хранилища на соответствии некоторым из стандартов доверия к электронным хранилищам – о получении сертификата «электронной печати качества» DSA (теперь эта сертификация называется CoreTrustSeal – «базовая печать доверия»), после чего может быть проведен (внутренний) аудит на соответствие ISO 16363.

Мой комментарий: *Давние партнеры - «Всемирная система данных» (World Data System,* https://www.icsu-wds.org/*) Международного совета по науке (International Council for Science, ICSU,* https://www.icsu-wds.org/*) и «Электронная печать качества» (Data Seal of Approval, DSA) – создали новый сертификационный орган CoreTrustSeal (*https://www.coretrustseal.org/about/*). CoreTrustSeal предлагает заинтересованным сторонам проведение сертификации базового уровня на основе положений и процедур «Базовых требований к доверенным хранилищам данных» (Core Trustworthy Data Repositories Requirements, см.* https://www.coretrustseal.org/wp-content/uploads/2017/01/Core_Trustworthy_Data_Repositories_Requirements_01_00.pdf*), совместно подготовленных DSA и WDS. Этот универсальный каталог требований отражает ключевые характеристики доверенных хранилищ и является кульминацией сотрудничества между DSA и WDS, направленного на слияние их систем сертификации. Новая сертификация заменила сертификации DSA и WDS.*

Зденек Хрушка (Zdeněk Hruška, Библиотека Моравии в Брно) говорил о важности определения расходов на содержание электронных хранилищ и об инструментах LIFE3 и KRDS2, используемых для расчета затрат. Финансовая устойчивость и способность хранилища находить бюджетные альтернативы имеют решающее значение с точки зрения его репутации (см. ISO 16363, п.3.4 «Финансовая устойчивость»). Модели затрат поддерживают такую способность, равно как и способность принимать решения, основанные на различных вариантах расходования средств. И хотя использовать некоторых из моделей затрат непросто (требуется время и кадровые ресурсы), однако преимущества этого очевидны. В конце концов, проведение внутреннего аудита на соответствие одному из стандартов доверенных хранилищ также является затратным по ресурсам, но получаемая от этого отдача неоспорима.

Золтан Люкс (Zoltán Lux) из Национальных Архивов Венгрии представил иную точку зрения на сертификации электронных хранилищ, поскольку венгерское хранилище не сертифицировано на соответствие международным стандартам доверенных хранилища, но в данный момент оно стремится соответствовать лишь национальному законодательству и требованиям к ИТ-безопасности. В Венгрии делается акцент на управление рисками, с тем, чтобы затрачиваемые ресурсы не оказались более дорогостоящими, чем

потенциальный ущерб. Интересно, что после того, как выступили другие докладчики, г-н Люкс признал, что им тоже пора задуматься о сертификации в соответствии с международно признанными стандартами, такими как CoreTrustSeal, Nestor Seal и ISO 16363. Похоже, что обмен информацией и проведение встреч на международном уровне приносят пользу, а обмен опытом имеет решающее значение для развития профессионального сообщества.

Катарина Томкова (Katarína Tomková) из словацкого Центрального архива данных (Centrálny dátový archív, CDA, http://cda.kultury.sk/) рассказала о целях этого проекта, об опыте проведения аудита в прошлом, а также о планах на будущее. Поскольку обязанность проводить аудит была изначально заложена в проект, то в 2014 году CDA прошёл внешний аудит «предварительной сертификации» на соответствие требованиям ISO 16363 и также был сертифицирован по стандарту ISO 27001. Были планы сертификации на соответствие DSA, но в связи с тем, что эта система сертификации была заменена на сертификацию CoreTrustSeal, хранилище CDA сейчас обдумывает свои дальнейшие шаги.

ЗМІСТ