ПЕРЕДМОВА

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

У публікації «Современный микрографический архив» розповідається, що сучасний архів утримує документи на паперовому, електронному і мікрографічному носіях одночасно, де кожна форма носія вирішує свої завдання для забезпечення оперативного доступу і використання інформації.

У публікації «Современные решения для библиотек» розповідається, що сьогодні бібліотеки значно розширили коло носіїв інформації і все більше поширення отримують електронні книги, аудіо- та відео-носії. В той же час, для забезпечення надійного довготривалого збереження бібліотечних фондів, поза конкуренцією залишаються мікрофіші і мікроплівка.

У публікації «Проект «ДНК документа»: Основные риски для сохранения электронных доказательств» наведено попередні дані опитування фахівців у рамках проекту "ДНК документу".

У публікації «США: Новый «Архивный канон»» наведено публікації з архівної тематики, які читачі вважають найбільш важливими.

У публікації «Евросоюз: Утвержден стандарт EN 419241-1 «Доверенные системы, поддерживающие подписание на сервере – Часть 1: Требования по безопасности»» розповідається, що ТС 224 Європейського інституту стандартів CEN затверджений остаточний варіант частини 1 стандарту EN 419241. Наведено стислу характеристику.

У публікації «Стандарты Казахстана по вопросам управления документами и информацией» наведено перелік стандартів Республіки Казахстан з питань управління документами та інформацією.

У публікації «Ответ на вопрос коллеги: Рекомендации ВНИИДАД и контейнерные форматы» надано рекомендації щодо використання контейненрних форматів для збереження електронних файлів.

У публікації «Андрей Пищиков, HPE: “Модель потребления ИТ предприятиями Украины не будет полностью облачной”» розповідається про роботу в Україні компанії Hewlett Packard Enterprise після її реорганізації.

У публікації «Конференция IDC Security Roadshow 2017» розповідається про питання управління ризиками та організаційні заходи щодо зниження ступеню загроз розглянуті в Києві на конференції IDC Security Roadshow 2017.

У публікації «Digital October 2017 – международный форум по кибербезопасности» розповідається про міжнародний форум з кібербезпеки що проходив у лютому 2017 року в Москві.

У публікації «Узнай что в облаке?» розповідається, що хмари стали новою нормою життя і попит на їхні послуги зростає.

СОВРЕМЕННЫЙ МИКРОГРАФИЧЕСКИЙ АРХИВ

Источник: http://ecm-journal.ru/docs/Sovremennyjj-mikrograficheskijj-arkhiv.aspx

Авторы: Сергей Елизаров, Дмитрий Ляховой *ООО "АКТЕК XXI"*

Проблема сохранения и доступности информации

Сегодня документы являются важнейшим информационным ресурсом и интеллектуальным результатом любого рода деятельности человека. В правовом обществе документы имеют не только информационное, но и юридическое значение, подтверждая имущественные, социальные и другие права граждан и юридических лиц. В документах аккумулируется, хранится и передается потомкам национальное, научное, культурное и историческое наследие.

За десятилетия успешной и плодотворной работы предприятиями накоплены огромные объемы документов, которые необходимо надежно хранить и иметь возможность использовать. К ним относятся архивы конструкторской, технологической документации, нормативно-технических документов, профильные библиотеки эксплуатационных документов, лицензионная документация, отчеты по НИОКР, обзоры и сравнительные анализы, кадровый и бухгалтерский архивы. Необходимость долговременного хранения этих документов определяется как их безусловной ценностью и, часто, уникальностью представленной в них информации, так и соответствующими положениями законодательства.

Необходимым условием сохранения и развития интеллектуального потенциала, конечно, является доступность книг, исторических материалов и прочих представляющих ценность документов для широкой аудитории. Огромный объем информации накоплен в библиотечных фондах научных заведений, библиотек, архивов и музеев. Заметная часть документов представлена в малом количестве, часто единственным экземпляром. К сожалению, подавляющее большинство хранимых документов выполнено на бумажных носителях, которые, даже при щадящем обращении и аккуратном хранении становятся хрупкими и желтеют после 3-10 лет использования. Многие из них, по причине старения, находятся в таком состоянии, что даже однократное обращение к документу может привести к его порче. Необходимость сохранения этих документов, так же как и необходимость обеспечения доступности информации, содержащейся в них, очевидна для каждого, кому небезразлично свое будущее.

Таким образом, проблема сохранения и доступности информации, преобразования бумажных документов в другие, более надежные и/или более доступные формы, сегодня чрезвычайно остро стоит в современном обществе.

Хранение информации на цифровых носителях

Не будет преувеличением сказать, что на сегодняшний день наилучшей формой оперативного хранения информации является цифровая форма. Т.е. хранение документов на магнитных лентах, магнитных дисках, магнитооптических дисках или оптических дисках. Такой архив документов компактен, обеспечивает скоростной доступ к информации из любой точки мира, простоту управления и поиска, одновременную работу с документом многими пользователями, очень гибкую настройку при практически неограниченном объеме хранимой информации. Заметим, что перечисленные выше преимущества достигаются не только высокотехнологичным оборудованием и развитым программным обеспечением, но и правильно выбранной формой организации электронного архива и формата записи данных.

Однако, как средство долговременного (от 10 до 100 и более лет) хранения, электронный архив имеет существенные недостатки:

Зависимость от выбранного цифрового носителя. Цифровые носители обновляются каждые 5-10 лет, и через 10-20 лет вы вряд ли найдете устройство, способное прочитать ваш CD, DVD или HDD, как сегодня компьютер, способный прочитать 5.25' дискету или перфокарту.

Срок гарантированного хранения. Для распространенных сегодня CD, DVD, HDD и прочих носителей срок гарантированного хранения не превышает 5-10, в исключительных случаях, 20 лет.

Зависимость от используемого программного обеспечения и формата данных. Программное обеспечение обновляется каждые 3-5 лет. Меняются кодировки, форматы данных, методы представления информации. Немногим дольше поддерживаются устаревшие программные продукты. Даже если через 10-20 лет вы найдете ту программу, в которой был создан сохраненный файл, сможете ли вы запустить ее на новом компьютере? Определенно нет.

Гарантия соответствия оригиналу. Вы уверены, что файл сохранен. Но, есть ли гарантия, что файл не был случайно или умышленно изменен? Возможно, он был испорчен вирусами. Возможно, никто этого не заметил. Такую вероятность никогда нельзя полностью исключать, если речь идет о цифровых носителях. По этой причине цифровая форма не может приниматься как подлинник документа и по ГОСТ статусом подлинника не обладает.

Хранение информации на микроформах

Таким образом, цифровая форма, несмотря на ее неограниченные возможности в части оперативной работы с документами, средством долговременного хранения информации служить не может.

Как средство надежного долговременного хранения информации наилучшими возможностями обладает микрографическая форма: рулонный или форматный микрофильм.

Микрографический архив позволяет преодолеть рассмотренные выше недостатки электронного архива, как средства долговременного хранения данных:

- Хранение данных на микроформах очень консервативно, смена форматов носителей практически не происходит. Документы, перенесенные на микропленку 50 лет назад, могут быть легко воспроизведены сегодня, завтра и в будущем.

- Срок гарантированного хранения микроформ составляет 100 и более лет.

- Микроизображение геометрически подобно изображению оригинала документа и не связано с какими-либо цифровыми форматами данных. Не требует для воспроизведения сложных устройств. При необходимости микроизображение может быть прочитано даже с помощью лупы.

- Современные фотографические материалы обеспечивают высокую степень геометрического и полутонового подобия микроизображения оригиналу. По ГОСТ 13.1.101-93 микрофильм имеет статус подлинника.

Микрографические технологии сегодня

Если раньше микрографические архивы развивались независимо от электронных архивов, то сегодня наблюдается значительное взаимное проникновение цифровых и микрографических технологий.

Так, с появлением сканеров микроформ технология микрофильмирования получила дополнительные возможности. Сегодня для любого пользователя не составит проблем перевести в электронный вид даже очень старые документы, записанные на микропленку. Многие конструкторские бюро восстанавливают старые архивы, переводя их на электронные носители. Учитывая фактор затребованности, и большие сроки хранения микроформ, такие работы можно проводить постепенно, что еще раз подтверждает экономическую эффективность микрографических архивов.

COM технология (расшифровывается как Computer Output Microfilm), т.е. технология вывода на микропленку цифровых данных, позволила хранить в микрографическом архиве электронные документы, минуя бумажную форму. COM-системы имеют высокий фактор редуцирования и скорость обработки документов. COM технология позволяет автоматически создавать образы документов, используя неформализованные данные с компьютерных систем. COM-системы сравнивают с принтером, с одним отличием, что печать осуществляется на микрофотоноситель. Также как и принтер, COM-система может быть использована в сетевом режиме, и за счет большой производительности обслуживать одновременно несколько сетей.

Активно предлагаемые сегодня гибридные системы представляют собой совмещенные комплекты оборудования сканирования документов (получение электронного образа) и печати микрофильмов. Такие системы, как правило, пишут на 16/35 мм рулонный фильм с достаточно высокой скоростью ввода для документов всех форматов от A0 до A6. Гибридные

системы решают одновременно проблемы создания архивов для оперативного и долговременного хранения информации.

Современный архив: бумага, электронный документ и микроформа

Таким образом, современный архив содержит документы на бумажном, электронном и микрографическом носителях одновременно, где электронная форма решает задачи оперативного доступа и использования информации, бумажный носитель служит для фиксации юридической и правовой составляющей работы, а микрографический архив решает задачи долговременного хранения информации, в том числе создания страхового фонда документации, который представляет особую ценность для предприятия-владельца в чрезвычайных и критических ситуациях.

Рис. 1. Современный архив: бумага, электронный документ и микроформа.

Блок-схема современного архива, содержащего документы на бумажном, электронном и микрографическом носителях, приведена на рис. 1. Исходные документы формируются как бумажном, так и в электронном виде. Бумажные документы для оперативного использования сканируются на широкоформатных, книжных или поточных сканерах и вводятся в систему электронного документооборота. Если необходимый срок хранения бумажного документа превышает 3-5 лет, то документ переводится в микрографическую форму с помощью микрофильмирующей системы и

помещается в микрографический архив. В случае, когда предполагается, достаточно частое использование документа, одновременно с микрофильмированием производится сканировании документа. Наиболее удобно выполнять такое преобразование с помощью гибридной системы. Для просмотра документов на микроформе и получения бумажных копий с микроформы применяются читальные и читально-копировальные аппараты. Для быстрого перевода микроформ в электронный вид используют специализированные сканеры микроформ. Документы, существующие в электронном виде и требующие долговременного хранения, могут быть сохранены на микроформу с помощью COM-системы. Отметим, что микрофильмирующие камеры, гибридные и COM-системы требуют применения проявочной машины для фиксации изображения на микропленке.

В приведенной на рис. 1 блок-схеме архив микроформ является логически необходимой составляющей современного архива, решающей задачи долговременного (от 5 до 100 и более лет), надежного хранения информации, в котором на системном уровне решены проблемы качества и подлинности хранимой информации. Кроме того, такой микрографический архив технологически интегрирован в систему бумажного и электронного документооборота.

Заключение

Сегодня мир вновь обратился к апробированной и надежной технологии долговременного хранения информации – микрографии, теперь существенно усовершенствованной и обогащенной новыми возможностями. Микрографическими архивами широко пользуются государственные структуры, государственные и коммерческие банки, национальные и публичные библиотеки, государственные архивы, научные и проектные учреждения, страховые компании, военные ведомства и т.д. Любые данные на микроформах могут быть оперативно переведены в электронную форму, а данные, записанные в электронном виде, могут быть “распечатаны” на микрографический носитель, минуя бумажную форму представления. Правительства многих стран мира законодательно утвердили подлинность документов снятых на микрофильм, их юридическая сила приравнена к оригиналу.

Таким образом, микрографический архив сегодня – это единственный путь, обеспечивающий долговременное (от 5 до 100 и более лет) хранение информации, в котором на уровне системного подхода решены проблемы надежности, качества и подлинности хранимой информации. Подробнее: http://ecm-journal.ru/docs/Sovremennyjj-mikrograficheskijj-arkhiv.aspx

СОВРЕМЕННЫЕ РЕШЕНИЯ ДЛЯ БИБЛИОТЕК

Источник: http://www.storage-systems.ru/solve/libraries/

Библиотека (от греческого «книга» и «место хранения») – это учреждение, которое собирает и хранит произведения печати и письменности для общественного пользования, а также осуществляет справочно-библиографическую работу. Первые библиотеки появились более 4500 лет назад на Древнем Востоке, это были коллекции глиняных табличек, папирусы, клинописные таблички, позже им на смену пришли книги. Сегодня библиотеки значительно расширили круг носителей информации – все большее распространение получают электронные книги, использование аудио- и видео-носителей, сохранение библиотечных фондов на микрофишах и микропленках.

Бесспорно, **заменить бумажную книгу невозможно**. Электронная версия способна дополнить бумажный оригинал, но лишь дополнить, а не заменить. Электронная версия – это способ представления информации, имеющий свои преимущества, и сегодня многие библиотеки мира предлагают электронные книги читателям.

Итак, в чем же состоят **преимущества электронных книг**?

• Это удобно: с электронным вариантом даже очень редкой книги может работать любое количество человек – так обеспечивается **публичный доступ** к изданиям.

• Это мобильно: за электронной книгой не надо идти в библиотеку, доступ к электронной книге может получить любой читатель, независимо от его местонахождения – очевидно **удобство использования**.

• Благодаря **автоматизированному поиску** по электронной базе данных, значительно экономится время, затрачиваемое на поиск книги, а, как следствие, время читателей и работников библиотек.

• При использовании электронных копий **оригиналы** книг **сохраняются** в целости в книгохранилищах.

Таким образом, сканирование документов и книг с целью создания электронных копий является одной из важнейших задач библиотек во всем мире. Помимо сканирования бумажных документов актуально сканирование микроформ, на которых сохранена часть библиотечных фондов.

Другой серьезной задачей библиотек является создание и наполнение страхового фонда редких книг и документов, представляющих безусловную историческую и культурную ценность. Наиболее надежным и проверенным временем носителем документации страхового фонда является микроформа. Технически информация на микроформы переносится прямым фотокопированием оригинала или посредством вывода цифрового образа оригинала на микроформу.

Современное оборудование позволяет легко, быстро и надежно решить проблемы сканирования любых бумажных книг и документов, а также вопросы создания, поддержки и модернизации электронных библиотек. Основные и незаменимые помощники в этом деле – **профессиональные сканеры**, современные модели которых позволяют преобразовать в электронный вид практически любой документ.

Книжные сканеры предназначены для сканирования книг и других брошюрованных документов. Большинство книжных сканеров – планетарные: сканирующая головка расположена "сверху" на значительном удалении от сканируемого документа, что обеспечивает повышенную сохранность оригиналов. Использование современных моделей книжных сканеров позволяет значительно повысить сохранность оригиналов, благодаря очень деликатному обращению с ними. Особенно это актуально при сканировании уникальных, редких и ветхих книг, старых рукописей, частично поврежденных или порванных, ценных архивных документов. Работа с такими материалами требует не только предельной аккуратности, но и специального оборудования, гарантирующего сохранность оригинала в процессе сканирование и высокое качество копии. При использовании современных книжных сканеров тысячи книг могут быть переведены в электронный вид, при этом электронные копии испорченных оригиналов или

оригиналов нестандартной формы могут быть отмасштабированы и распечатаны в качественные бумажные копии.

Широкоформатные сканеры используются для сканирования карт, чертежей и других документов большого формата (к примеру, форматов A0 и A1). Современные модели обеспечивают высочайшее разрешение и точную цветопередачу даже при компактных размерах.

Поточные сканеры используются для работы с несброшюрованными документами любого формата (от A6 до A3), обеспечивая высокоскоростное сканирование (до 320 страниц в минуту), при минимальном вмешательстве оператора.

Для работы с библиотечными микроформами предназначены **сканеры микроформ**, позволяющие переводить в электронный вид микрофиши и микропленки всех распространенных форматов, в том числе и в полностью автоматическом режиме, и **читальные аппараты микроформ**, предназначенные для просмотра микроформ читателем без помощи компьютера.

Компания АКТЕК XXI предлагает новейшие технологии сканирования и микрофильмирования для создания, поддержки и модернизации цифровых и микрографических архивов. Мы предлагаем оборудование от ведущих мировых производителей (Microbox, Zeutschel, Wicks & Wilson, Houston Fearless, Mekel, Extek и других) и готовые решения для всех видов библиотек: национальных, публичных, специальных, университетских, школьных. Осуществляем полный цикл работ по поставке, установке, наладке, калибровке и сервисному обслуживанию оборудования. Мы всегда открыты для общения. Если вы хотите приобрести оборудование или просто получить консультацию, свяжитесь с нами, **мы обязательно вам поможем**!

ПРОЕКТ «ДНК ДОКУМЕНТА»: ОСНОВНЫЕ РИСКИ ДЛЯ СОХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Источник: сайт проекта http://www.allourideas.org/recorddna/results?page=1
Автор: Наташа Храмцовская

В одном из постов на блоге (см. http://rusrim.blogspot.ru/2017/06/blog-post_23.html) уже рассказывалось о международном проекте «ДНК документа», который выполняется под контролем Университетского колледжа Лондона, и о проводимых в его рамках опросах специалистов.

К настоящему времени собрана большая коллекция вариантов ответа на вопрос «Каковы основные риски для сохранения электронных документов как доказательств во времени?» (см. http://www.allourideas.org/recorddna/results?page=1) К 25 июня участники опроса около 8 тысяч раз проголосовали за 55 ответов, и, на мой взгляд, достаточно интересно проанализировать, что же в итоге получается.

Конечно, участники проекта ещё дадут свой анализ, а пока я хочу предложить Вам собственную сводку результатов. Меня интересовала не статистика голосования, а те проблемы, которые волнуют коллег. Я постаралась сгруппировать варианты ответов по тематическим блокам, объединив похожие. Вот что в итоге получилось:

Разработка стратегий и систем

- Неспособность выбрать подходящую стратегию в момент проектирования систем.
- Неудачная архитектура унаследованных систем, не позволяющая провести надлежащим образом перенос электронных доказательств в новые системы.
- Слепая вера в какую-то одну «универсальную» технологию (например, в квалифицированные подписи, блокчейн и т.п.).
- Обеспечение непрерывности при переходе от бумажных к электронным документам.

Выявление документов

- Перегрузка информацией в неорганизованной среде – как отыскать документы, которые могут служить доказательствами?
- Неспособность выявить и идентифицировать документы из-за их расползания по системам, в связи отсутствием согласованной информационной архитектуры или недостаточной поддержки со стороны руководства и заинтересованных сторон.
- Проблема установления самого факта существования документов.

- Отсутствие «единой версии истины» - что является истинным документом?

Объёмы документации, сроки хранения и уничтожение

- Экспоненциальный рост объёмов электронных документов, особенно тогда, когда нет ясного понимания, что нужно сохранять, а что следует уничтожить.
- Неспособность организовать своевременное уничтожение переставших быть нужными документов.
- Тенденция хранить всё.
- Несистематическое проведение уничтожения, сложность хранения электронных документов.

Целостность, аутентичность, безопасность

- Утрата контекста – неспособность понять, как и зачем документы создавались и использовались.
- Утрата взаимосвязей между данными – электронный документ обычно состоит из взаимосвязанных компонент, и эти связи со временем могут быть нарушены.
- Вирусы, криптолокеры, трояны, фишинг – злонамеренные силы, атакующие или портящие доказательную базу.
- Сбои оборудования.
- Порча данных.
- Целостность – насколько она важна в мире, где существует электронная судебно-криминалистическая экспертиза?
- Неспособность обеспечить непрерывность деловой деятельности.
- Утрата ключей к зашифрованным данным.
- Возможные прорывы в криптографии, способные поставить под угрозу доверие к существующим документам и системам, которые существенно полагаются на криптографию.

Изменение, устаревание, конверсия / миграция, пригодность к использованию

- Доступ к устаревшим форматам, системам, устройствам хранения; постепенное ветшание ранних носителей информации.
- Проблема доступа по мере изменения программных и аппаратных платформ.
- Адаптация к меняющимся с течением времени технологиям. Можно это сделать один раз, однако тяжело раз за разом адаптироваться к новым технологиям.
- Миграция – имеем ли мы дёло со всё тем же оригинальным документальным доказательством после его миграции?
- Доступность – будем ли мы знать о существовании документов, если доступность не будет поддерживаться во времени?
- Теряется смысл содержания документов, если те представляют собой слишком «зашифрованный» ответ на другие документы, связь с которыми потеряна.

- Утрата сведений о том, где именно хранится важнейшая информация.
- Утрата технических знаний и навыков, необходимых для извлечения информации из устаревших систем и унаследованных документов.

Проблемы деловой деятельности, экономические проблемы

- Нехватка ресурсов.
- Отсутствие приоритетов.
- Отсутствие опыта и знаний.
- Отсутствие взаимодействия между создателями документов, руководством и ИТ-персоналом.
- Отсутствие согласованности между различными частями одной организации.
- Ситуация, когда создание документов более не рассматривается как неотъемлемая часть деловых процессов, и воспринимается как дополнительный, часто неприоритетный вид деятельности.
- Осознание создателями документов того, что в будущем эти документы могут стать для них источником неприятностей, особенно если будут использованы средства для их сведения и совместного анализа в электронном виде.
- Осмысленность метаданных – нужно автоматизировать процессы их создания.
- Определение ценности документов как доказательств: в буквальном смысле определение отдачи на инвестиции на их сохранение (независимо от вида и формата).
- Затраты и время, необходимые не передачу электронных документов в другие системы или на преобразование в иные форматы.

Правовые проблемы

- Право владения – когда владельцами частей документа являются различные стороны, компании-разработчики ПО, авторы, поставщики услуг облачного хранения.
- Правовая неопределенность в отношении подходящих методов обеспечения долговременной сохранности электронных доказательств (особенно в странах континентального права), что открывает возможности для оспаривания доказательств в будущем. Примерами могут служить обеспечение долговременной сохранности электронных цифровых подписей и подписанных такими подписями документов.
- Facebook и другие крупные корпорации захватывают контроль над доказательной базой, и она уже не находится под контролем государства.

США: НОВЫЙ «АРХИВНЫЙ КАНОН»

Источник: блог ArchivesNext http://archivesnext.com/?p=4456
Автор: Наташа Храмцовская

Заметка известного американского архивиста-блоггера Кейт Теймер была опубликована 26 июня 2017 года на её блоге ArchivesNext.

В прошлом году я попросила Вас, читателей своего блога, как архивистов, так и представителей других профессий, назвать те публикации по архивной тематике, которые Вы считаете важнейшими (см. http://archivesnext.com/?p=4118).

Я немного упорядочила Ваши предложения, и они размещены ниже, – но подозреваю, что у нас всё еще есть пробелы в списке «важнейших публикаций современности». Итак, пришло время для второго этапа обсуждения - что, по-вашему, нужно включить в Новый Архивный Канон, или, говоря проще, что именно следует прочесть каждому архивисту? Какие публикации оказали на Вас наибольшее влияние? Как обычно, благодарю Вас за Ваш вклад!

Мой комментарий: *Как мне кажется, нашим ученым, специалистам-практикам, педагогам и студентам тоже может быть интересен список публикаций, которые их американские коллеги считают наиболее значимыми. Во многих случаях гиперссылки выводят на полные тексты.*

Список публикаций:

Джефферсон Бейли (Jefferson Bailey) **«Неуважение фондов: Пересмотр принципов упорядочения и описания в архивах изначально-электронных документов»** (Disrespect des Fonds: Rethinking Arrangement and Description in Born-Digital Archives), «Архивный журнал» (Archive Journal), лето 2013 года, http://www.archivejournal.net/issue/3/archives-remixed/disrespect-des-fonds-rethinking-arrangement-and-description-in-born-digital-archives/

Лори Бейти (Laurie Baty) **«Фотографии – не обои»** (Photographs are not Wallpaper) - нужна ссылка!

«Архивы, документация и институты социальной памяти: Эссе с Сойеровского семинара» (Archives, Documentation, and Institutions of Social Memory: Essays from the Sawyer Seminar), под ред. Френсиса Блуина (Francis X. Blouin, Jr.) и Уильяма Розенберга (William G. Rosenberg), 2006 год, https://muse.jhu.edu/book/351

«Архивные истории: Факты, мифы и написание истории» (Archive Stories: Facts, Fictions, and the Writing of History), под ред. Антуанетты Бёртон (Antoinette Burton), 2006 год, https://www.dukeupress.edu/archive-stories

Мишель Кэсвел (Michelle Caswell) и Марика Сифор (Marika Cifor), **«От прав человека до феминистской этики: Радикальная эмпатия в архивах»** (From Human Rights to Feminist Ethics: Radical Empathy in the Archives),

журнал Archivaria, весна 2016 года, http://archivaria.ca/index.php/archivaria/article/view/13557

Скотт Клайн (Scott Cline), **«"Тебя покроют облака пыли, поднятой [везущими дары] верблюдами": Неформальный пакт между заинтересованными сторонами и усилия в области архивного дела»** ('Dust Clouds of Camels Shall Cover You': Covenant and the Archival Endeavor), журнал «Американский архивист» (American Archivist), осень/зима 2012 года, http://americanarchivist.org/doi/pdf/10.17723/aarc.75.2.03193j1517858r34

Терри Кук (Terry Cook), **«Прошлое является прологом: История архивных идей с 1898 года, и будущий сдвиг парадигм»** (What is past is prologue: a history of archival ideas since 1898, and the future paradigm shift), Archivaria №43 (1997), стр. 17-63, http://archivaria.ca/index.php/archivaria/article/view/12175/13184

Терри Кук (Terry Cook) и Джоан Шварц (Joan M. Schwartz), **«Архивы, документы и власть: От (постмодернистской) теории к (архивной) практике»** (Archives, Records, and Power: From (Postmodern) Theory to (Archival) Performance). «Архивная наука» (Archival Science), том 2, №3-4 (2002), стр. 171–185, https://www.scribd.com/document/137086706/Archives-Records-And-Power-From-Postmodern-Theory-to-Performance

Терри Кук (Terry Cook), **«Концепция архивных фондов в посткастодиальную эпоху: Теория, проблемы и решения»** (The Concept of the Archival Fonds in the Post-Custodial Era: Theory, Problems and Solutions),журнал Archivaria, весна 1993 года, http://arqtleufes.pbworks.com/w/file/fetch/94919891/COOK%20TERRY_The%20Concept%20of%20the%20Archival%20Fonds.pdf

Терри Кук (Terry Cook), **«Свидетельство, память, идентичность и сообщество: Четыре меняющихся архивных парадигмы»** (Evidence, memory, identity, and community: four shifting archival paradigms), «Архивная наука» (Archival Science), июнь 2013 года, http://link.springer.com/article/10.1007/s10502-012-9180-7

Терри Кук (Terry Cook), **«Модная чепуха или профессиональное возрождение: Постмодернизм и архивная практика»** (Fashionable Nonsense or Professional Rebirth: Postmodernism and the Practice of Archives), журнал Archivaria, весна 2001 года, http://archivaria.ca/index.php/archivaria/article/view/12792

Брюс Диастайн (Bruce Dearstyne), **«Лидерство и менеджмент программ управления документами и архивами: Стратегии успеха»** (Leading and managing archives and records programs: strategies for success), 2008 год, https://www.amazon.com/Leading-Managing-Archives-Records-Programs/dp/1555706150

Жак Деррида (Jacques Derrida), **«Архивная лихорадка: Запечатление по Фрейду (религия и постмодернизм)»** (Archive Fever: A Freudian Impression (Religion and Postmodernism)), 1998 г.,

https://www.amazon.com/Archive-Fever-Freudian-Impression-Postmodernism/dp/0226143678

Жак Деррида (Jacques Derrida), **«Зарождение, генеалогия, жанры и гений: Секреты архива»** (Geneses, Genealogies, Genres and Genius The Secrets of the Archive), 2006 г., https://www.amazon.com/dp/B0071I536K/ref=cm_sw_su_dp

Джаррет Дрейк (Jarrett M. Drake) **«Бунтующие граждане: Сомнительная практика создания полицейских документов в Новом Орлеане после урагана Катрина, и её последствия для прав человека»** (Insurgent citizens: the manufacture of police records in post-Katrina New Orleans and its implications for human rights), «Архивная наука» (Archival Science), октябрь 2014 года, http://link.springer.com/article/10.1007/s10502-014-9224-2

Мишель Дюшен (Michel Duchein), **«Теоретические принципы и практические проблемы, связанные с принципом уважения фондов в архивной науке»** (Theoretical Principles and Practical Problems of Respect des fonds in Archival Science), журнал Archivaria, лето 1983 года, http://archivaria.ca/index.php/archivaria/article/viewFile/12648/13813

Лючиана Дюранти (Luciana Duranti), **«Архив как место»** (Archives as a Place), «Исследования в области архивных и социальных наук: журнал междисциплинарных исследований» (Archives & Social Studies: A Journal of Interdisciplinary Research), том 1, №0 (март 2007 года), http://archivo.cartagena.es/doc/Archivos_Social_Studies/Vol1_n0/07-duranti_archives.pdf

Лючиана Дюранти (Luciana Duranti), **«Дипломатика: Новое применение старой науки»** (Diplomatics: New Uses for an Old Science), журнал Archivaria, лето 1989 года, http://archivaria.ca/index.php/archivaria/article/viewFile/11567/12513

Урсула Франклин (Ursula Franklin) **«Реальный мир технологий»** (The Real World of Technology), 1992 год, https://www.amazon.com/dp/088784636X/ref=cm_sw_su_dp

Элси Фриман (Elsie Freeman), **«Покупая дырки диаметром в четверть дюйма: Получение общественной поддержки через результаты работы»** (Buying Quarter Inch Holes: Public Support Through Results, журнал «Среднезападный архивист» (Midwestern Archivist), 1985 год, https://minds.wisconsin.edu/handle/1793/45944 (прямая ссылка https://minds.wisconsin.edu/bitstream/handle/1793/45944/MA25_1and2_8.pdf)

Элизабет Фридман (Elisabeth Friedman), **«Анти-архив? Фильм Клода Ланцмана «Шоа» и дилемма представления Холокоста»** (The anti-archive? Claude Lanzmann's Shoah and the dilemmas of Holocaust representation), http://www.academia.edu/2060148/THE_ANTI-ARCHIVE_CLAUDE_LANZMANNS_SHOAH_AND_THE_DILEMMAS_OF_HOLOCAUST_REPRESENTATION

Тимоти Гилфойл (Timothy J. Gilfoyle), **«Архивные материалы о проститутках: Проблемы и возможности документирования истории**

сексуальности» (Prostitutes in the Archives: Problems and Possibilities in Documenting the History of Sexuality), «Американский архивист» (American Archivist), лето 1994 года, http://americanarchivist.org/doi/pdf/10.17723/aarc.57.3.p74tr646p6r530lv

Анна Гийланд (Anne Gilliland) и Сью МакКемиш (Sue McKemmish), **«Создание инфраструктуры для архивных исследований»** (Building an Infrastructure for Archival Research), «Архивная наука» (Archival Science), декабрь 2004 года, http://link.springer.com/article/10.1007/s10502-006-6742-6 (полный текст: https://www.academia.edu/18650385/Building_an_Infrastructure_for_Archival_Research)

Тим Голлинз (Tim Gollins), **«Экономное обеспечение долговременной сохранности: предотвращение бессмысленных процессов! (Простые малые шаги, которые позволяют очень далеко продвинуться в деле обеспечения долговременной сохранности электронных материалов)»** (Parsimonious preservation: preventing pointless processes! (The small simple steps that take digital preservation a long way forward), 2009 год, http://www.nationalarchives.gov.uk/documents/information-management/parsimonious-preservation.pdf

Марк Грин (Mark A. Greene) и Денис Мейснер (Dennis Meissner), **«Больше продукции, меньше процессов: Пересмотр традиционной архивной обработки»** (More Product, Less Process: Revamping Traditional Archival Processing), «Американский архивист» (American Archivist), осень/зима 2005 года, http://www.archivists.org/prof-education/pre-readings/IMPLP/AA68.2.MeissnerGreene.pdf

Джеральд Хэм (Gerald Ham), **«Архивный [передний] край»** (The Archival Edge), «Американский архивист» (American Archivist), январь 1975 года, http://americanarchivist.org/doi/pdf/10.17723/aarc.38.1.7400r86481128424

Верн Харрис (Verne Harris), **«Архивы и правосудие: Южноафриканская перспектива»** (Archives and Justice: A South African Perspective), 2013 год, http://saa.archivists.org/store/archives-and-justice-a-south-african-perspective-pdf/3691/

Питер Хёртл (Peter Hirtle), **«Архивная аутентичность в электронную эпоху»** (Archival Authenticity in a Digital Age), в сб.: «Аутентичность в электронной среде» (Authenticity in a Digital Environment), CLIR, 2000 год, стр.8-23, https://www.clir.org/pubs/reports/pub92/pub92.pdf

Рэндал Джимерсон (Randall C. Jimerson), **«Сила архивов: Память, подотчётность и социальная справедливость»** (Archives Power: Memory, Accountability, and Social Justice), 2009 год, http://saa.archivists.org/store/archives-power-memory-accountability-and-social-justice/1354/

Рэндал Джимерсон (Randall C. Jimerson), **«Архивы для всех: Профессиональная ответственность и социальная справедливость»** (Archives for All: Professional Responsibility and Social Justice),

«Американский архивист» (American Archivist), осень/зима 2007 года, http://americanarchivist.org/doi/pdf/10.17723/aarc.70.2.5n20760751v643m7

Элизабет Каплан (Elisabeth Kaplan), **«Мы – то, что мы собираем; мы собираем то, чем мы являемся: Архивы и формирование самобытности»** (We Are What We Collect, We Collect What We Are: Archives and the Construction of Identity), «Американский архивсит» (American Archivist), весна/лето 2000 года, http://conservancy.umn.edu/bitstream/handle/11299/42433/1/kaplan_we_are_what.pdf

Эрик Кетелаар (Eric Ketelaar), **«Архивные храмы, архивные тюрьмы: Режимы власти и защиты»** (Archival Temples, Archival Prisons: Modes of Power and Protection), «Архивная наука» (Archival Science), №2, 2002 год, http://home.hccnet.nl/e.ketelaar/ArchivalTemples.pdf

Эрик Кетелаар (Eric Ketelaar), **«Негласные правила игры: Смысл архивов»** (Tacit Narratives: The Meanings of Archives), «Архивная наука» (Archival Science) 2001 год, https://deepblue.lib.umich.edu/handle/2027.42/41812 (прямая ссылка: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/41812/10502_2004_Article_359685.pdf)

Мишель Лайт (Michelle Light) и Том Хайри (Tom Hyry) **«Колофоны [*выходные данные, сведения о подготовке документа – Н.Х.*] и аннотации: Новые направления развития научно-справочного аппарата»** (Colophons and Annotations: New Directions for the Finding Aid), «Американский архивист» (The American Archivist), осень/зима 2002 года, том 65, №2, стр 216-230, https://doi.org/10.17723/aarc.65.2.l3h27j5x8716586q (прямая ссылка: http://americanarchivist.org/doi/pdf/10.17723/aarc.65.2.l3h27j5x8716586q)

Джон Макдональд (John MacDonald), **«Управление документами в современном офисе: Наведение порядка на диком пограничье»** (Managing Records in a Modern Office: Taming the Wild Frontier), журнал Archivaria, №29, весна 1995 года, http://archivaria.ca/index.php/archivaria/article/view/12069/13047

Сью МакКемиш (Sue McKemmish), **«Свидетельства обо мне»** (Evidence of Me), «Австралийский библиотечный журнал» (The Australian Library Journal), 1996 год, http://www.tandfonline.com/doi/abs/10.1080/00049670.1996.10755757

Эрнст Познер (Ernst Posner) **«Архивы штатов США»** (American State Archives), 1964 год, https://www.amazon.com/dp/B0000CMIYG/ref=cm_sw_su_dp

Эрнст Познер (Ernst Posner) **«Архивы и общественный интерес: Избранные эссе»** (Archives and the Public Interest: Selected essays), 1967 год, https://www.amazon.com/Archives-Public-Interest-Ken-Munden/dp/B0000CHD20/ref=mt_hardcover

Эрнст Познер (Ernst Posner) **«Архивы в древнем мире»** (Archives in the Ancient World), 1972 год, http://www.hup.harvard.edu/catalog.php?isbn=9780674437005

Ли Рейн (Lee Raine) и Барри Велман (Barry Wellman), **«Сетевое общество: Новая социальная оперативная система»** (Networked: The New Social Operating System), 2014 год, https://www.amazon.com/dp/0262526166/ref=cm_sw_su_dp

Питер Скотт (Peter Scott) **«Концепция документной группы: Обоснование отказа от неё»** (The Record Group Concept: A Case for Abandonment), «Американский архивист» (The American Archivist), октябрь 1966 года, том 29, №4, стр. 493-504, http://americanarchivist.org/doi/10.17723/aarc.29.4.y886054240174401

Джоан Шварц (Joan M. Schwartz), **««Правдивые и точные документы»: Фотография, архивы и иллюзия контроля»** ("Records of Simple Truth and Precision": Photography, Archives, and the Illusion of Control), журнал Archivaria, осень 2000 года, http://www.archivaria.ca/index.php/archivaria/article/view/12763/13951

Люси Зухман (Lucy Suchman), **«Делая работу видимой»** (Making Work Visible), журнал Communications of the ACM, сентябрь 1995 года, http://guzdial.cc.gatech.edu/hci-seminar/uploads/1/Suchman's+Making+Work+Visible.pdf

Чиаран Трейс (Ciaran B. Trace), **«То, что задокументировано, никогда не является просто «тем, что произошло»: Делопроизводство в современной организационной культуре»** (What is Recorded is Never Simply 'What Happened': Record Keeping in Modern Organizational Culture), «Архивная наука» (Archival Science), 2002 год, https://www.ischool.utexas.edu/~cbtrace/pubs/CBT_ArchScience_2002.pdf

Рето Чан (Reto Tschan), **«Сопоставление взглядов Дженкинсона и Шелленберга на экспертизу ценности»** (A Comparison of Jenkinson and Schellenberg on Appraisal), «Американский архивист» (American Archivist), осень/зима 2002 года, http://americanarchivist.org/doi/pdf/10.17723/aarc.65.2.920w65g321770611

С.Уильямс (S. Williams) **«Малоизвестные грани архивной работы: Если мы хотим, чтобы наш труд уважали, мы сами должны выше его ценить»** (Implications of Archival Labor: If we want respect for our labor, we need to value it more), апрель 2016 года, https://medium.com/on-archivy/implications-of-archival-labor-b606d8d02014#.wyb8jlp3y

Марк Вольф (Mark D. Wolfe), **«Не только «зелёные» корпуса: Изучение влияния парадокса Джевонса на экологичность архивной практики»** (Beyond ''green buildings:'' exploring the effects of Jevons' Paradox on the sustainability of archival practices), 2011 год, http://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1015&context=ulib_fac_scholar

Элизабет Якель (Elizabeth Yakel), **«Архивное упорядочение и описание»** (Archival Representation), «Архивная наука» (Archival Science), 2003 год,

https://deepblue.lib.umich.edu/bitstream/handle/2027.42/41831/10502_2004_Article_5139967.pdf?sequence=1

Элизабет Якель (Elisabeth Yakel), **«Защоренное и незашоренное мышление: Архивная справочная служба на рубеже столетий»** (Thinking Inside and Outside the Boxes: Archival Reference Services at the Turn of the Century), журнал Archivaria, №49, 2000 год, http://archivaria.ca/index.php/archivaria/article/viewFile/12742/13927

Кейт Теймер (Kate Theimer)

Мой комментарий: К сожалению, для доступа к отдельным ресурсам могут понадобиться анонимайзеры: (Ничего не поделаешь – запуганные русскими хакерами малообразованные американские сисадмины частенько блокируют доступ с российских IP-адресов).

ЕВРОСОЮЗ: УТВЕРЖДЕН СТАНДАРТ EN 419241-1 «ДОВЕРЕННЫЕ СИСТЕМЫ, ПОДДЕРЖИВАЮЩИЕ ПОДПИСАНИЕ НА СЕРВЕРЕ – ЧАСТЬ 1: ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ»

Источник: сайт LinkedIn http://bit.ly/2sPlMKX
http://rusrim.blogspot.com/2017/07/en-419241-1-1.html

Краткое сообщение французского специалиста Франка Леруа, директора по технологиям доверенных сервисов компании DOCAPOST, эксперта и редактора стандартов CEN/ETSI и AFNO

На встрече в Эссене (Essen), Германия, эксперты рабочий группы WG17 по профилям защиты в контексте защищённых устройств для создания подписи (Protection profiles in the context of SSCD) технического комитета TC 224 Европейского института стандартов CEN утвердили окончательный вариант части 1 стандарта EN 419241:

EN 419241-1 «Доверенные системы, поддерживающие подписание на сервере – Часть 1: Требования по безопасности» (Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements).

Стандарт EN 419241-1 определяет два уровня уверенности (assurance):

- Уровень уверенности в исключительном контроле 1 (SCAL1):
  - Ключи подписания используются, с низким уровнем уверенности, под исключительным контролем подписанта;
  - Использование уполномоченным подписантом его ключа для подписания обеспечивается с помощью протокола SSA, авторизующего подписанта.
- Уровень уверенности в исключительном контроле 2 (SCAL2):

- Ключи подписания используются, с высоким уровнем уверенности, под исключительным контролем подписанта;
- Использование уполномоченным подписантом его ключа для подписания обеспечивается на основе полуаналитической модели (Semi analytic model, SAM) с помощью данных активации подписи (Signature Activation Data, SAD), которые представляются подписантом с использованием протокола активации подписи (Signature Activation Protocol, SAP), с тем, чтобы сделать возможным использование соответствующего ключа подписания.

Стандарт позволит создать удаленную систему электронного подписания / проставления электронных печатей для усиленного и квалифицированного уровней.

После трёх лет разработки и интенсивных дискуссий эксперты наконец-то пришли к консенсусу (*замечу, что новый стандарт заменит ранее действовавшие европейские технические спецификации CEN/TS 419241:2014 «Требования по безопасности к доверенным системам, поддерживающие подписание на сервере» - Security Requirements for Trustworthy Systems Supporting Server Signing*).

Я хотел бы поблагодарить всех экспертов-членов рабочей группы из Великобритании, Германии, Франции, Италии, Испании, Дании и Швеции.

Франк пишет: Количество одобривших стандарт национальных членов: 100.000%, настоящий успех!

Было высказано несколько замечаний, поэтому экспертной группе придётся подготовить финальную версию с тем, чтобы принять их во внимание, и за этим последует публикация документа. Публикация ожидается к концу года.

Последним шагом является утверждение соответствующих профилей защиты (часть 2 стандарта – это EN 419241-2:2017 «Доверенные системы, поддерживающие подписание на сервере – Часть 2: Профиль защиты для квалифицированных устройств создания подписи для подписания на сервере» (Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing).

СТАНДАРТЫ КАЗАХСТАНА ПО ВОПРОСАМ УПРАВЛЕНИЯ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ

Автор: Наташа Храмцовская http://rusrim.blogspot.com/2017/06/

По ходу изучения стандартов ряда стран, я столкнулась с тем, что нигде не смогла найти актуального списка стандартов Республики Казахстан

по тематике управления документами и информацией. В итоге я составила собственный список (естественно, без претензий на полноту):

- СТ РК 1042-2001 «Организационно-распорядительная документация» (утратил силу)
- СТ РК 1037-2001 «Делопроизводство и архивное дело. Термины и определения»
- СТ РК 1237-2004 «Система стандартов по информации, библиотечному и издательскому делу. Документы на бумажных носителях. Общие технические требования к архивному хранению»
- СТ РК ИСО 5127-2007 «Информация и документация - Словарь»
- СТ РК ИСО 15489-1-2007 «Информация и документация - Оперативный учет. Часть 1: Общие положения»
- СТ РК ИСО 15489-2-2007 «Информация и документация - Оперативный учет. Часть 2: Руководство»
- СТ РК ИСО 22310-2010 «Информация и документация. Руководство для разработчиков стандартов, устанавливающих требования к управлению документами»
- СТ РК ГОСТ Р ИСО 23081-1-2010 «Информация и документация. Процессы управления записями. Метаданные для записей. Часть 1. Принципы»
- СТ РК ИСО 23081-2-2010 «Информация и документация. Метаданные для управления записями. Часть 2. Вопросы концепции и реализации»
- СТ РК ИСО 14721-2010 «Космические системы передачи данных и информации. Открытая архивная информационная система. Эталонная модель»
- СТ РК ISO 30300-2012 «Информация и документация. Системы менеджмента для записей. Основные положения и словарь»
- СТ РК ISO 30301-2012 «Информация и документация. Системы менеджмента для документов. Требования»

Также отмечу ещё несколько стандартов, которые меня по тем или иным причинам заинтересовали:

- СТ РК ISO 12651.1-2012 «Менеджмент электронной документации. Словарь. Часть 1. Графическое представление документов»
- СТ РК ИСО/ТО 10013-2008 «Руководящие указания по документированию системы менеджмента качества»
- СТ РК DSP-IS 0101-2016 «Совместимые облака»
- СТ РК DSP-IS 0102-2016 «Архитектура для управления облаками»
- ПСТ РК 49-2015 «Электронное здравоохранение - Электронный паспорт здоровья. 1-часть»
- ПСТ РК 50-2015 «Электронное здравоохранение - Электронная медицинская запись. 2-часть»

- СТ РК ГОСТ Р 34.10-2015 «Информационная технология - Криптографическая защита информации - Процессы формирования и проверки электронной цифровой подписи»
- СТ РК ГОСТ Р 34.11-2015 «Информационная технология - Криптографическая защита информации - Функция хэширования»

ОТВЕТ НА ВОПРОС КОЛЛЕГИ: РЕКОМЕНДАЦИИ ВНИИДАД И КОНТЕЙНЕРНЫЕ ФОРМАТЫ

Автор: Наташа Храмцовская
Источник: http://rusrim.blogspot.com/2017/06/blog-post_86.html

Вопрос: Я ознакомился с некоторыми методическими рекомендациями (http://archives.ru/documents/methodics.shtml***). С точки зрения форматов, для долгосрочного хранения рекомендуется использовать:***

- ***XML (включая XSD/XSL/ XHTML),***
- ***PDF/A-1 (ISO 19005-1) (*.pdf)***
- ***PDF/A-2 (ISO 19005-2:2011) (*.pdf)***

и при этом формировать контейнер электронного документа (zip-папку), которая содержит:

- ***файл электронного документа в формате архивного (долгосрочного) хранения;***
- ***файлы электронных подписей;***
- ***файлы проверки электронных подписей, подтверждающие положительный результат проверки электронной подписи.***

Как Вы думаете, стоит ли «закладываться» на эти рекомендации при проектировании системы?

Ответ: Приведенные Вами рекомендации содержатся в следующих документах, разработанных ВНИИДАД в 2013 году:

- Рекомендации по комплектованию, учету и организации хранения электронных архивных документов в архивах организаций, http://archives.ru/sites/default/files/rekomendation-vniidad-edoc-org-2013.pdf
- Рекомендации по комплектованию, учету и организации хранения электронных архивных документов в государственных и муниципальных архивах, http://archives.ru/sites/default/files/rekomendation-vniidad-edoc-arch-2013.pdf

Рекомендации, на мой взгляд – это всё-таки или система высокоуровневых принципов и требований, и/или описание конкретной технологии, которая опробована на практике. К сожалению, в данных документах детали проведения работы по формированию контейнера не

описаны, практического опыта приема/передачи на архивное хранение электронных документов в таких контейнерах нет, судебной практики тоже нет. Кроме того, ни слова не сказано о том, что с этими контейнерами затем делать бедному архиву! Контейнеры можно рассматривать и как единицы хранения, и всего лишь как средство передачи документов в архив. В общем, как мне кажется, опираться на упомянутые методические документы при организации практической работы пока преждевременно.

Очень важно, что под данными рекомендациями нет никакой правовой почвы, и Вы можете использовать их исключительно на свой страх и риск. Однако ровно на тех же основаниях – на свой страх и риск - Вы можете использовать и авторитетные международные стандарты и рекомендации!

Отмечу, что в мире вполне успешно используется несколько подходов к передаче электронных документов на архивное хранение. Там, где считают важной возможность передавать, обрабатывать и/или хранить каждый архивный документ (или группу документов, например, дело) вместе со всеми его метаданными и прочей информацией как единый защищённый электронный объект, – и таких архивов сейчас большинство, – используются контейнерные форматы. Есть разные форматы такого рода – это и ZIP, и XML, и форматы собственной разработки. Внутренняя структура информации в контейнере у каждого своя; она выбирается в зависимости от поддерживаемых функциональных возможностей, и разнообразие здесь огромное. Есть, например, страны, где контейнерные форматы изначально используются для создания и оперативной работы с документами в делопроизводстве, а впоследствии документы в этом же виде уходят и на архивное хранение. Длительно работающие электронные архивы обычно где-то раз в пять лет пересматривают структуру своих контейнеров в связи с изменением потребностей и технологий.

Важен следующий момент: при длительном архивном хранении формируются дополнительные заверенные копии документов в новых форматах, создаются дополнительные метаданные – соответственно, встает вопрос о том, как дополнять защищённые контейнеры этой новой информацией.

Есть иные варианты, когда способ передачи ориентирован не на отдельный документ, а сразу на большой массив документов, без использования контейнеров. Базовый стандарт электронной архивации OAIS (ISO 14721) в качестве основных понятий использует «сдаточный информационный пакет» (SIP), «архивный информационный пакет» (AIP) и «дистрибутивный информационный пакет» (DIP), однако не настаивает на том, чтобы это были физические сущности (т.е. они могут существовать как логические, виртуальные объекты).

Контейнерные форматы не всегда технически применимы – они, например, скорее всего, не помогут в случае, когда на архивное хранение придётся принимать большие и сложные базы данных.

Коротко отмечу также следующее:

- Уже существует 4 основных варианта форматов семейства PDF/A, каждый из которых имеет свои подварианты, и у каждого – свои достоинства и недостатки. По мере появления новых вариантов базового формата PDF тут же будут появляться и новые разновидности формата PDF/A;
- PDF/A годится не для всех документов;
- Для определенных видов документов открытых форматов для долговременного хранения просто нет (например, для САПР-чертежей). В то же время для технических документов существует своя, специализированная версия формата PDF для длительного хранения.
- Если оригиналы были подписаны усиленными подписями, их всё равно придётся хранить в оригинальном формате (возможно, изготавливая дополнительные заверенные копии в иных форматах для удобства использования и для обеспечения долговременной сохранности).

Главная рекомендация следующая: документы длительного и постоянного срока хранения нужно (если возможно) изначально создавать в форматах, пригодных для долговременного хранения!

Принципиальная ориентация на контейнерные форматы – вполне нормальный выбор. Однако о том, что это будет за контейнер, и каким образом информация в нём будет структурирована, придётся подумать самостоятельно.

Наверное, стоит сразу «заложиться» на то, что первые варианты контейнеров окажутся не совсем удачными, и первые партии таких контейнеров со временем придётся переформатировать в контейнеры более позднего образца. Этого бояться не нужно, важно лишь позаботиться о том, чтобы подобное переформатирование было возможно без ущерба для целостности, аутентичности, юридической значимости и доказательной силы документов.

АНДРЕЙ ПИЩИКОВ, HPE: «МОДЕЛЬ ПОТРЕБЛЕНИЯ ИТ ПРЕДПРИЯТИЯМИ УКРАИНЫ НЕ БУДЕТ ПОЛНОСТЬЮ ОБЛАЧНОЙ»

Источник: http://ko.com.ua/andrej_pishhikov_hpe_model_potrebleniya_it_predpriyatiyami_ukrainy_ne_budet_p

Компания Hewlett Packard Enterprise в особом представлении не нуждается, хотя была образована лишь в ноябре 2015 года. После разделения Hewlett-Packard на две независимые структуры, она унаследовала бизнес, связанный с корпоративными решениями HP. Сегодня мы предлагаем

вашему вниманию интервью с Андреем Пищиковым, руководителем украинского Представительства HPE. И наш первый вопрос о том, как начался для компании третий квартал.

Мы наблюдаем ощутимый рост сегмента enterprise, сказывается отложенный спрос предыдущих лет. Ряд приостановленных проектов начинают реализовываться. В целом весьма позитивный взгляд на ближайшее время.

Можете ли вы охарактеризовать текущую ситуацию на глобальном и локальном рынках за те полтора года, что произошли после разделения компании HP?

Сегодня мы – две независимые компании. Компания HP Inc., унаследовавшая знакомый всем логотип, является нашим глобальным партнером. К слову, это разделение прошло быстро и совершенно безболезненно, если учитывать его масштабы.

Компания HPE приняла решение оптимизировать портфель продуктов и услуг, а также откорректировать стратегию, чтобы быстрее реагировать на изменения в ИТ-индустрии, учитывая наступление эпохи Industry 4.0, IoT, больших данных и тп.

Вследствие этого, было принято решение о выделении подразделения Enterprise Service в отдельную компанию и ее дальнейшем слиянии с Computer Sciences Corporation (CSC). Более 50% акций новообразованной компании, получившей название DXC Technology, будут принадлежать HPE. Аналогичные преобразования происходят и с нашим подразделением программного обеспечения. Продукты для телеком-решений останутся в портфеле HPE, весь остальной портфель станет частью компании Micro Focus, где HPE также будет иметь долю чуть более 50%.

Помимо выделения подразделений, мы установили стратегические партнерства с Arista, Mesosphere, Dropbox и некоторыми другими и имеем план поглощения компаний: на сегодняшний день наш портфель пополнился компаниями Aruba, SGI, Simplivity, Cloud Cruiser, Niara, Nimble Storage.

Следуя глобальным тенденциям, таким как IoT, рост потребления ИТ-сервисов из облаков компаниями, изменения требований к качеству услуг и т.п. - стратегия нашей компании состоит в том, чтобы максимально соответствовать современным потребностям наших клиентов и одновременно адресовать новые точки роста ИТ рынка.

А как эти глобальные тенденции влияют на стратегию HPE на рынке Украины?

Краеугольный камень стратегии HPE - Hybrid IT, что особенно актуально для украинского рынка. Мы считаем, что предприятия не перейдут полностью на облачные модели потребления ИТ, а будут использовать как собственные ИТ-ресурсы, так и облачные сервисы. Портфель предложений HPE поможет нашему заказчику максимально реализовать такой подход.

У HPE есть конвергентные системы BladeSystem, компонуемая инфраструктура Synergy, системы для высокопроизводительных вычислений

High Performance Computing. В 2016 г. затраты на R&D таких решений возросли примерно на 30% по сравнению с предыдущим годом. В рамках нашей стратегии по развитию Hybrid IT установлено партнерство с компаниями, предоставляющими публичные облака, - Amazon, Microsoft, Dropbox и многими другими, которые, возможно, менее известны в Украине, но активно представлены в Западной Европе и Северной Америке. Если говорить про направление высокопроизводительных вычислений, то с приобретением Silicon Graphics International (SGI) мы получили доступ как к ее технологиям, так и к важному сегменту рынка. Недавнее поглощение компании Simplivity, которая специализируется на гиперконвергентных решениях, так же серьезно укрепило наш портфель и в этом сегменте.

Не могли бы вы объяснить, чем было вызвано выделение тех двух подразделений из бизнеса HPE, что отошли CSC и Micro Focus?

При таком широком портфеле продуктов, от мобильных устройств до систем HPC с большим набором сервисов, компании было очень тяжело проводить изменения с той скоростью, с которой меняется рынок. Поэтому, чтобы увеличить маневренность компании, было принято такое решение. Так, например, подразделению Enterprise Services, нацеленному на предоставление прежде всего аутсорсинговых услуг, будет гораздо проще освободиться от давления конкретных технологических преференций, чтобы стать более динамичным, а объединение с CSC сделает его более заметным на рынке.

Чем отличается выделенное подразделение Enterprise Services от того направления консалтинговых услуг, которое осталось?

В сферу деятельности Enterprise Services входило в основном все, что связано с ИТ-аутсорсингом для больших компаний. Если говорить о консалтинговых услугах в составе HPE, то это ИТ-консалтинг, то есть помощь ИТ-подразделениям клиентов (а также другим жестко связанным с ИТ структурой элементам) трансформироваться в соответствии с требованиями бизнеса, изменениями внешней и внутренней среды.

Консалтинговые услуги сейчас находятся в зоне ответственности недавно созданного подразделения технологических сервисов HPE PointNext, наличие которого отражает важность роли сервисов в новой стратегии компании и отвечает за предоставлении услуг трех типов: Advisory and Transformation - дают возможность компаниям разработать и создать технологическую дорожную карту, отвечающую их бизнес-целям; Professional Services помогают заказчику реализовать намеченные трансформационные инициативы; Operational Services (HPE Flexible Capacity и Datacenter Care) поддерживают работоспособность и функционирование систем и сред клиента на необходимом для бизнеса уровне.

Тема облаков не теряет своей актуальности. Каков подход к этим технологиям компании в целом? Вы уже упомянули о партнерстве с основными игроками на этом рынке. Нужно ли это понимать так, что между вами нет конкуренции?

Мы являемся лидерами рынка Hybrid IT в мире. Наша главная задача – помогать ИТ соответствовать требованиям бизнеса в каждом конкретном моменте времени, используя для этого самые современные подходы и технологии. Поэтому, если в определенный момент времени появляется потребность в использовании облачной составляющей, то наше партнерство с ведущими мировыми игрокам в области публичных облаков, позволит клиенту оптимально и без проблем ее получить.

Нет ли опасений, что облачная составляющая, вытеснит какие-то ваши системы или решения?

Возможно такой риск и присутствует, но, наше мнение, основанное на опыте других стран и регионов, что скорее будет перераспределение от того, что называется IT on premise к Hybrid IT, когда часть ИТ-сервисов потребляется предприятием от внешнего поставщика: сервис-провайдера. Наша стратегия в этом – как сотрудничество с глобальными компаниями провайдерами публичных облаков так и поиск и инициализация локальных партнеров, cloud service providers. Для таких компаний мы можем путем выработки совместной модели продвижения продуктов, сервисов, интеграции команд по продажам и т. п., предложить новые возможности в расширении их классического бизнеса, например для телеком-компаний.

Сервис-провайдеры – это будущее ИТ-рынка. Компании, которые предоставляют услуги, становятся наибольшими потребителями ИТ в том сегменте, в котором мы работаем. Если посмотреть на страны Западной Европы, то доля сервис-провайдеров в некоторых из них составляет 70% ИТ рынка.

Такие локальные компании сервис-провайдеры во многих случаях имеют преференции на местных рынках, что безусловно определяет наш приоритет в работе с ними.

Нашими партнерами для облачных и гибридных решений также являются американские и европейские телеком операторы и ряд финансовые компаний. Здесь также есть специальные программы по сотрудничеству, к примеру, Cloud 28+, когда сервис провайдеры, наши партнеры, объединены в одно сообщество и имеет возможность обмениваться наработками и лучшими практиками. Это позволяет не только опосредованно расширять свой портфель предложений и географию присутствия, но так же значительно сокращать time to market таких сервисов.

То есть вы полагаете, что в будущем сохранятся не три – пять крупных облачных оператора, а будут тысячи упомянутых выше провайдеров облачных услуг?

На сегодня говорить о глобальной консолидации провайдеров облачных сервисов не приходится ввиду современных геополитических процессов и определенных технологических ограничений. Кроме этого, по многим причинам наличие собственной ИТ-системы является жизненно необходимым для некоторых типов клиентов, и не все еще могут использовать облака. Стратегия HPE Hybrid IT и наш портфель продуктов и

услуг, а также партнерские программы отражает эту реальность. Например, наши партнерские соглашения с компанией Arista, которая занимается программно-управляемыми облачными сетями (Software Driven Cloud Networking). Крупнейшие ЦОДы в Америке (Google, Microsoft, Facebook) используют технологию Arista, которая присутствует в нашем портфеле и является комплементарной технологией в нашей модели Hybrid IT.

А решения этой компании не вытесняют какие-то ваши традиционные предложения?

Есть определенные пересечения, но они незначительные. Более важно, что решения дополняют друг друга в области сетей ЦОД. Мне кажется, что к подобного рода системам вскоре придут и крупные украинские компании имеющие собственные ЦОД.

Так что Arista является примером взаимовыгодного партнерства.

Но Hybrid IT - это только одна часть стратегии компании. Второй существенной частью, безусловно, является все, что связано с IoT. Сейчас “Интернет вещей” выглядит как концепция, и, если угодно, на практике реализуемая в основном больше стартапами, чем большими корпорациями. Стандарты в этой области еще формируются. Да, есть концепция, есть модели применения, наработки, протоколы, есть определенные успехи, но наличие IP-адреса или чипа в носимом устройстве без соответствующей экосистемы не является достаточным. Необходимы отработанные бизнес-сценарии с явным экономическим эффектом.

Мы не хотим конкурировать в производстве чипов для носимых устройств или в производстве самих таких устройств. Для этого есть специализированные компании, которые, кстати, являются нашими партнерами. В этих областях мы сотрудничаем с мировыми лидерами – General Electric, National Insturments, Intel и другими. У нас же есть IoT-платформа, которую клиенты используют для обработки данных, получаемых от соответствующих датчиков и устройств

Также в контексте IoT стоит упомянуть Aruba, технологическом лидере в области беспроводных сетей. Ее разработки хорошо укладываются в концепцию IoT. Так, сервисы определения местоположения пользователя Wi-Fi и информация о нем могут быть использованы для операционных или бизнес-сценариев.

Об IoT говорят все, однако не все понимают, что с этим делать, поскольку рынок еще, скажем так, не оформился. Но те проекты, который уже были реализованы HPE, показывают, что уже сейчас в рамках общего движения можно выделить некоторые нишевые потребности в рамках IoT, к примеру, вычисления «на границе». Не всегда выполнять обработку данных от IoT целесообразно в ЦОД или в удаленном облаке. Есть множество сценариев, когда предварительную обработку данных рационально выполнять на устройствах, расположенных в местах генерирования данных. Именно для этого у нас есть специальное предложение HPE Edgeline IoT Systems.

Если коснуться традиционных решений HPE, которые есть в портфеле компании, таких как серверы, СХД, сетевое оборудование, все это остается?

Конечно, весь набор решений по-прежнему остается, и эти решения востребованы. Ведь когда мы говорим о Hybrid IT, то это включает и классический ЦОД. Наш сбалансированный продуктовый портфель помогает построить оптимальную для бизнеса конфигурацию. Он включает решения как HPC, так и серверы индустриального стандарта, и мы очень хорошо себя чувствуем в этих сегментах. И серверы, и СХД требуют определенной программной поддержки, для того чтобы стать конвергентной инфраструктурой. У нас есть программный продукт HPE OneView для консолидированного управления серверами, системами хранения данных и сетевым оборудованием, который позволяет перейти к конвейерному развертыванию новых сервисов и ускорить трансформацию классической инфраструктуры в облачную (инфраструктура как сервис, IaaS) и переход к гибридным облакам. 3PAR, XP, Superdome, серверы x86, системы начального уровня - всё это сегодня востребовано нашим рынком.

Все что вы описали и на чем концентрируется сегодня компания требует серьезных инвестиций в R&D. Какое место они занимают в бизнесе HPE на фоне выделения ряда подразделений?

HPE держит курс на инновационность, и общее финансирование R&D в 2016 г. было увеличено примерно на 30%. Те активы, которые мы сейчас приобретаем, соответствуют нашей стратегии, дополняя имеющиеся компетенции и увеличивая конкурентоспособность в наших целевых сегментах.

Отвечая на ваш вопрос об исследованиях и разработках хотел бы отметить одно из направлений, что сегодня разрабатывается HPE Labs: Memory-Driven Computing, архитектура вычислительных систем ближайшего будущего. Пример тому - The Machine. В прошлом ноябре на ежегодном мероприятии HPE Discover в Лондоне уже был показан действующий прототип. Это направление, по которому мы активно работаем и видим в нем будущее индустрии.

Вы упомянули в контексте публичных облаков Dropbox, который ориентируется прежде всего на малый и средний бизнес. Есть ли в вашем портфеле предложения и для этих сегментов, или все же вы фокусируетесь только на корпоративных пользователей, как может сложиться впечатление исходя из названия компании?

Безусловно, такие решения всегда были и остаются в нашем портфеле. Наибольшие изменения, на самом деле, происходят именно в сегменте SMB, потому что малый и средний бизнес быстрее реагирует на появление новых технологий, новых концепций, новых стилей потребления.

В корпоративном сегменте в последнее время также наблюдаются серьезные изменения - кризис вынуждает компании смотреть на ИТ как на инструмент получения конкурентных преимуществ.

Если говорить о том, что значит SMB для HPE, то глобально – это около 40% бизнеса, в Украине – порядка 50%.

Имеется ли для SMB какой-то специальный портфель предложений?

Да, есть серверные предложения, есть СХД, которые ориентированы на SMB-сегмент, есть и сервисные предложения. Это все остается в нашем портфеле, и никто полностью смещаться в корпоративный сегмент не собирается. Так же наблюдаем, что в Украине ряд крупных предприятий приобретают продукты из портфеля SMB по финансовым соображениям. Большая доля в рассматриваемом сегменте, кстати, принадлежит госсектору, в том числе из-за государственных инициатив по децентрализации.

А как построена партнерская сеть для сегмента SMB?

Без партнеров продажа в этот сегмент для HPE невозможна. Рынок серьезно трансформировался за последние годы. Количество проектов в сегменте SMB значительно снизилось и резко возросла конкуренция. Как результат, критерием успеха становится экспертиза и возможность решить задачи заказчика как на бизнес, так и на операционном уровне. Стоит отметить отдельно такой сегмент как региональный госсектор. С процессом децентрализации в регионах появились бюджеты и, как результат, новые ИТ-проекты.

Усилилась ли конкуренция в партнерской среде?

Она усилилась прежде всего потому, что рынок сжался. За два года мы очень сильно, примерно на 60%, сократили партнерскую сеть. Сокращение было вынужденным, чтобы снизить конкуренцию в нашем сегменте партнерских продаж и заодно повысить уровень экспертизы нашего канала. Объективно, у нас были ценовые войны, потому что минимальная цена была основным и, иногда, единственным критерием, который был интересен потребителю.

Сейчас мы перестраиваем нашу партнерскую модель и для нас более интересны компании, которые обладают широкими компетенциями, у которых присутствует business value sales, которые умеют работать с нашим программными приложениями и приложениями наших альянс партнеров. У нас много новых партнеров, разрабатывающих собственное ПО и решения на базе наших технологий. Дополнительно мы ищем своеобразную конвергенцию между компетенциями партнеров, используя их наработки и предложения, а также наш опыт работы с глобальными партнерами.

Да, остались традиционные задачи создания ИТ инфраструктуры, их никто не отменял, и партнерская сеть, которая решает эти задачи. Мы работаем с ними по-прежнему, но, тем не менее, сейчас стали более открытыми ввиду того, что компания готова рассматривать значительно больше вариантов сотрудничества, чем это было раньше.

Если до недавнего времени у нас был только один тип партнерства по типу реселлера, то сейчас их стало больше, и это соответствует потребностям рынка. Например, помимо реселлера, сейчас у нас активно появляются

партнеры со статусом «сервис провайдер» для компаний, предоставляющих услуги на наших решениях, «технологический партнер» для независимых производителей ПО, OEM партнер для построения аппаратно-программных решений на базе наших технологий.

Наше консалтинговое и сервисное подразделения, а также техподдержка готовы работать в более широкой сфере, с расширенным портфелем предложений, в том числе и как ресурс для наших партнеров.

И на самом деле задача не состоит в том, чтобы выиграть каждую сделку. Партнерская модель – это сбалансированная самообучающаяся система, способная эффективно адресовать точки роста.

По логике вещей, получается, что количество партнеров сейчас начинает расти. Мы сегодня активно развиваем партнеров. Однако в Украине успешность проекта по-прежнему определяется взаимоотношениями: ты должен знать человека, чтобы продавать. Но появляются, усиливаются, а где-то становятся очень заметными продажи именно за счет преимущества технологий, продуктов и обеспечения бизнес-ценностей для клиентов, которые были сформированы из точек роста. Причём с полным стеком продуктов и компетенций.

А в корпоративный сегмент продажи идут напрямую?

Мы не продаем продукты напрямую – всё равно здесь есть участие партнера. Это создает порядка 50 – 60% рынка.

А какова сейчас ситуация в локальном офисе, после всех происшедших преобразований?

С нашей точки зрения, несмотря на все сложности и проблемы, рынок Украины обладает существенным потенциалом для реализации которого требуется непосредственное присутствие в стране.

HPE офис в Украине после завершения всех трансформаций (выделения в отдельные юридические лица подразделений Enterprise Service и ПО) будет насчитывать около 90 сотрудников. Подразделения продаж, поддержки продаж, технологических сервисов (трансформированный в HPE PointNext) и тд не претерпели существенных изменений в штатном расписании.

КОНФЕРЕНІЯ IDC SECURITY ROADSHOW 2017

Источник: http://idcitsecurity.com/kyiv_ua

Конференція IDC Security Roadshow 2017 відбулася 17 лютого у НСК Олімпійський, м. Київ.

Про IDC

IDC - провідний постачальник інформації і консультаційних послуг, організатор заходів на ринках інформаційних технологій, телекомунікацій і споживчої техніки. IDC допомагає професіоналам IT, керівникам і інвесторам приймати обґрунтовані рішення про закупівлю техніки і вибір бізнес-стратегії. Понад 1100 аналітиків IDC в 110 країнах вивчають технології, тенденції і можливості галузі на світовому, регіональному та місцевому рівнях. Уже понад 50 років знання IDC допомагають клієнтам компанії у рішенні найважливіших завдань. IDC - дочірнє підприємство IDG, компанії, яка лідирує на світовому ринку IT-видань, досліджень і спеціалізованих заходів. Більш детальна інформація на нашому сайті www.idc.com.

На тлі зміни технологічної платформи, глибокого проникнення IT у всі бізнес-процеси, масового розповсюдження хмарних обчислень, корпоративної мобільності та інтернету речей, питання інформаційної безпеки виходять на перший план змушуючи компанії докорінно змінювати звичні підходи до ІБ. З третьорядного завдання IT департаменту Інформаційна Безпека перетворюється на стратегічну функцію, вимагаючи від CISO глибокого розуміння "більшої картини", проактивної участі у впровадженні інновацій, перегляді бізнес-процесів з врахуванням ризиків для ключових активів, формуванні корпоративної культури та вичерпному розслідуванні інцидентів.

Для українських компаній ситуацію загострюють геополітичні ризики та хронічне недофінансування навіть базових потреб. На цьогорічній конференції IDC Security Roadshow 2017 в Києві 17 лютого було розглянуто, як управляти ризиками у прив'язці до бізнес пріоритетів, які організаційні заходи можуть значною мірою знизити ступінь загроз, за рахунок чого можна суттєво скоротити термін виявлення та реакції на загрози, як забезпечити ефективний моніторинг загроз та захист від витоку даних, як діяти в разі інцидентів, провести розслідування та забезпечити своєчасне відновлення даних на дієздатність систем.

Ключові теми IDC Security Roadshow 2017

Стратегічне бачення завдань інформаційної безпеки

Захист пристроїв

Аналітика загроз і захист від шкідливих програм в епоху Третьої Платформи. Вихід за межі захисту, що базується на сигнатурах, для впровадження в інфраструктуру, що постійно розвивається, рішень безпеки наступного покоління

Ідентифікація як периметр

Ідентифікація вже стала новим периметром - чи усвідомлюють це у вашій компанії? Розвиток біометрії і поширення концепції BYOD; багатофакторна аутентифікація - обов'язкова умова для корпоративної мобільності.

Безпека, сфокусована на самих даних

Захист даних це комплексні процедури, пов'язані з управлінням і безпекою, які включають контроль над доступом і правами користувача, шифрування, політики і правила, а також корпоративна культура.

Ми поговоримо не тільки і не стільки про рішення та необхідність інвестицій в технології захисту інформації, скільки про клієнтів, партнерів та співробітників, бізнес-процеси та стратегічне бачення проблем ІБ в контексті перспектив розвитку підприємства, галузі, країни.

Детально розглядались питання

- Перестороги та реальні загрози пов’язані з порушенням конфіденційності, цілісності та доступності корпоративних даних
- Управління ризиками в часи турбулентності. Безпека критичних систем. Стратегія і тактика захисту в умовах кібер-війни
- Політики безпеки та корпоративна культура. Комунікація пріоритетів інформаційної безпеки для керівників та персоналу
- Перехід від фрагментарного та ситуативного реагування на інциденти до цілісного стратегічного плану дій. Аналіз вразливостей в реальному часі, прогнозування та пріорітизація ризиків. Автоматизація процесів та процедур в інформаційній безпеці.
- Нові завдання ІБ в контексті масового розповсюдження хмарних обчислень, корпоративної мобільності та інтернету речей

ПРОГРАМА:

09:30 **Вітальне слово від IDC**

Володимир Поздняков, регіональний менеджер IDC в Україні, Білорусі, Молдові, Грузії та Арменії

09:35 **IDC Keynote: Зміни пріоритетів інформаційної безпеки в умовах підвищеного ризику**

Олексій Проскура, програмний директор, ІБ, IDC CEE

Чому потрібно перестати розглядати безпеку тільки з точки зору інформаційних технологій? Чому традиційні підходи до безпеки бізнесу недієздатні в сьогоднішніх умовах підвищеного ризику? Які галузі інформаційної безпеки стають найбільш пріоритетними і які функції відділу ІБ потрібно розвивати? Ми запізнюємося, давайте разом подумаємо як надолужити згаяне.

10:00 **Дика природа кіберпростору. Принципи виживання**

Володимир Стиран, експерт з кібер-безпеки, ентузіаст спільноти інформаційної безпеки та етичний хакер

Як відомо, людина менша та повільніша майже за все на Землі, що здатне її з’їсти. Тому протягом еволюції нам довелося об’єднатися та навчитися використовувати інструменти для підсилення наших кволих кінцівок. Ця стратегія виявилася напрочуд успішною в боротьбі за

виживання в дикій природі, але нові загрози сучасності вимагають нового підходу. Чи ні?

10:25 **Трансформаційна програма кіберзахисту об'єктів критичної інфраструктури в Україні**

Олексій Янковський, President ISACA Kyiv Chapter

11:00 **Виставка партнерів,** Coffee Break.

11:30 **Сучасні загрози, або чому помер Анти-Вірус**

Сергій Невструєв, керівник запобігання загрозам, Східна Європа, Check Point Software Technologies Ltd**.**

Зловмисники стають все більш винахідливими в способах отримання доступу до корпоративних ресурсів. Маючи в розпорядженні інструменти для модифікації атаки, вони можуть обходити традиційні засоби інформаційного захисту. Тому вже сьогодні необхідні рішення, які будуть здатні виявляти та запобігати новим, невідомим досі загрозам.

11:55 **Безпека Інтернету речей і управління ризиками: з чого почати?**

Мирослав Міщенко, менеджер по роботі з корпоративними клієнтами в Україні та Білорусі, Fortinet

Інтернет речей є невід'ємною частиною 4ої промислової революції та відкриває багато можливостей для підприємств, але одночасно і підвищує ризики, пов'язані з безпекою. Організаціям необхідно враховувати цей фактор при побудові своєї стратегії інформаційного захисту. Кількість підключених пристроїв з кожним роком експоненціально зростає і комплексний підхід до забезпечення інформаційної безпеки дозволить мінімізувати загрози, які несе Інтернет речей.

12:20 **Ефективна політика безпеки – що вона означає і які витрати на неї?**

Марис Сперга, директор розвитку бізнесу Центрів Обробки Даних, Lattelecom

Безпека є однією з основних потреб кожної людини - як тільки людина знаходиться в небезпеці, вона відчуває стрес і концентрується тільки на ньому, до моменту, поки загроза не пропадає. Кожен з нас намагається убезпечитись, щоб зменшити вплив загроз на самих себе, але чи так само ми ставимося до бізнесу? Найголовніше розуміти, що може створювати ризик для безпеки, які можуть бути наслідки? Якщо інцидент уже стався, то як діяти в таких ситуаціях? У своїй презентації сьогодні я постараюсь знайти відповіді на питання - які дані оперують в бізнесі, як їх класифікувати всередині компанії, яку політику та інструменти необхідно використовувати що б ефективно знизити ризики для бізнесу.

12:45 **Активна кібер-безпека в сучасних реаліях України. Огляд методів захисту від невідомих та передових атак**

Михайло Кондрашин, технічний директор Trend Micro в країнах СНД, Trend Micro

Третя світова війна вже почалася. Ресурс, за який іде боротьба - інформація.

Ми всі, навкруги, говоримо про те, що кібер-атаки переросли в бізнес доступний непрофесіоналам. Бізнес, який приносить живі гроші. З досвіду України чітко видно – додаткову вартість кібер атакам надає політична ситуація навколо. А, атаки на українські інфраструктурні об'єкти, вже починають входити в звичку, тому в доповіді увага акцентована на питаннях виявлення, аналізу та нейтралізації сучасних прихованих направлених атак в режимі реального часу.

13:05 **There is no Security without Visibility**

Павло Сотников, керуючий Директор по Східній Європі, Кавказу та Центральній Азії, Qualys

Парадокс: на ринку інформаційної безпеки зараз величезна кількість різних засобів, кількість яких все збільшується і збільшується, але при цьому і кількість взломів також зростає з кожним роком. В чому причина? Чому інциденти продовжують відбуватися? У своїй доповіді я спробую відповісти на це питання. Також я спробую розповісти, як за допомогою безперервного моніторингу своєї інфрастурктури і контрагентів можна збільшити швидкість реагування на інциденти або зовсім виключити їх виникнення!

14:30 **Захист конфіденційної інформації в сучасному світі: зниження ризиків, захист інвестицій, технології DLP.**

Павло Назаревич, керівник напрямку Symantec в країнах СНД, компанія МОНТ УА, MONT GROUP

У сучасному світі цінність інформації дуже висока. Реалії такі, що в багатьох компаніях і організаціях інформація є основним активом і основною цінністю. У той же час інформація несе для організації ймовірність багатьох ризиків. Ті компанії, які освоїли процеси за класифікацією інформації, оцінці її цінності і ризиків, пов'язаних з нею, отримують величезні переваги. Більше того такі процеси значно знижують вірогідність успішної кібер атаки з використанням соціальної інженерії. Таким чином для кожної сучасної компанії і організації необхідно розробляти стратегію по класифікації інформації та у справах захисту від витоку цінної інформації. У доповіді будуть висвітлені технології та світові практики із впровадження рішення класу Data Loss Prevention, яка забезпечить наявність всіх необхідних інструментів по роботі з конфіденційною інформацією в організації (від класифікації та створення політик до активних превентивних дій)

14:50 **Результати аналізу недавніх атак і рекомендації щодо поліпшення захисту від сучасних загроз**

Олександр Іллюша, керівник служби технічної підтримки в Україні, ESET

Хто здійснює цілеспрямовані атаки?

Які найбільш вразливі місця в інфраструктурі?

Які можуть бути наслідки цілеспрямованих атак?

Хто винен в тому, що вас зламали?

Як поліпшити захист від сучасних загроз?

15:10 **Кібер-злочини: як виявити, зібрати докази та притягнути до відповідальності. Успішний досвід співпраці адвокатів та комп'ютерних криміналістів**

Сергій Чеховський, генеральний директор та співзасновник, EPOS

Микола Орлов, керуючий партнер, Law Offices of OMP

• Хіт-парад кібер-злочинів України або стрімке погіршення ситуації вже сьогодні

• Проблеми виявлення та притягнення до відповідальності IT Моріарті

• Докази – на чому зосередити зусилля або особливості доведення вини «ручок з клавіатурою»

• Профілактика кібер-злочинів або чому дешевше запобігти аніж виправляти

16:00 **Закриття конференції**

DIGITAL OCTOBER 2017 – МЕЖДУНАРОДНЫЙ ФОРУМ ПО КИБЕРБЕЗОПАСНОСТИ

Источник: https://runet-id.com/event/csf17/

7 февраля 2017 года на площадке **Digital October** в Москве прошел десятый «юбилейный» международный форум по кибербезопасности – **Cyber Security Forum 2017**. Форум является ключевой частью Недели безопасного Рунета, официальной российской серии мероприятий Международного Дня безопасного Интернета (Safer Internet Day).

Основная задача Форума – это обмен опытом и выявление лучших практик в сфере информационной безопасности (технологии, законодательство и решения).

Направления работы CSF 2017

Основная задача Форума – межотраслевой диалог и обмен опытом в области информационной безопасности, выявление лучших практик по направлениям: технологии, решения, законодательство, цифровая грамотность. Участники Форума приглашаются к обмену практическим опытом и обсуждению лучших практик в сфере защиты от угроз с использованием технологий.

Секции Форума посвящены программно-техническим, обучающим, юридическим вопросам безопасности в цифровой среде, проблемам законодательства и принятия решений, роли специалистов и пользователей в информационной, мобильной и кибербезопасности, формированию позитивной Интернет-среды и позитивного контента. В их работе приняли участие ведущие специалисты по кибербезопасности из интернет-индустрии

и смежных отраслей, представители профильных государственных и правоохранительных органов, эксперты в области позитивного контента, представители исследовательского и образовательного сообщества.

Cyber Security Forum – это отличная возможность перенять опыт экспертов в этой области, обменяться мнениями с коллегами, познакомиться с гуру отрасли.

Организаторы, партнеры и аудитория CFS 2017

Организатор Форума: РОЦИТ, **соорганизатор:** РАЭК.

Отраслевая поддержка Форума: ИРИ, КЦ, РСпектр, Российско-Британская торговая палата, Франко-российская торгово-промышленная палата. Форум проходил при поддержке Министерства связи и массовых коммуникаций РФ и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

К участию в Cyber Security Forum были приглашены: представители отрасли (лидеры рынка по направлениям: интернет, телеком, софт, IIoT, безопасность), профильных ассоциаций и объединений (РАЭК, ИРИ, КЦ, Ассоциация «Интернета вещей», ФРИИ, АПКиТ, РУССОФТ, ТПП), органов госвласти (Минкомсвязь, Госдума, Совет Федерации, Роскомнадзор, Роспечать, МВД, ФСБ), международные представители, отраслевые эксперты, представители СМИ и другие представители профильных организаций.

Подробнее о Safer Internet Day

Международный День безопасного Интернета (Safer Internet Day) – главное мировое событие, посвященное безопасному использованию Интернета и цифровых технологий. День безопасного Интернета отмечается с 2004 года и в настоящее время охватывает свыше 130 стран по всему миру. Международным организатором является сеть Центров безопасного Интернета Insafe.

В России официальные мероприятия Дня безопасного Интернета проводятся с 2008 года, и CSF 2017 – ключевой проект российской программы.

Форум является ключевой частью Недели безопасного Рунета, официальной российской серии мероприятий Международного Дня безопасного Интернета (Safer Internet Day), и пройдет точно в День безопасного Интернета.

В открытии CSF 2017 приняли участие: **Приезжева Антонина** (Роскомнадзор), **Ларина Екатерина** (Минкомсвязь России), **Сергей Гребенников** (РОЦИТ), **Сергей Плуготаренко** (РАЭК), **Зинина Ульяна** (Майкрософт), **Воробьев Андрей** (Координационный центр национального домена сети Интернет), **Гордеева Марина** (Фонд поддержки детей, находящихся в трудной жизненной ситуации), **Якушев Михаил** (ICANN). Спикеры обсудили наиболее актуальные вопросы кибербезопасности, обозначили существующие проблемы и тренды, проанонсировали последующие доклады.

“За 10 лет наш форум трансформировался: в самом начале своей истории форум назывался i-Safety. Сегодня форум представляет в совершенно ином виде - Cyber Security Forum- это площадка для обсуждения ряда вопросов, связанных с различными аспектами темы кибербезопасности в Рунете. Отдельно хотелось бы отметить, что интернет-индустрия Рунета – самый активный и развивающийся сегмент экономики страны. За последние несколько лет рынок вышел в лидеры по целому ряду направлений и показателей в Европе: самая большая аудитория, самые крупные компании, самый активный сегмент рекламы, четвертое место по объему инвестиций и пятое по обороту электронной торговли. В связи с этим, мы видим необходимость обсуждения вопроса безопасности индустрии для дальнейшего развития интернет-отрасли. Спикеры форума – это представители ключевых компаний и организаций, развивающих интернет, занимающихся вопросами кибербезопасности и не только. Я очень рад, что сегодня мы имеем возможность собраться здесь и обсудить такие важнейшие вопросы, как: цифровая грамотность, цифровая безопасность и суверенитет России, регулирование в области инфобезопасности и многие другие острые темы”, – сказал **Сергей Плуготаренко**, директор РАЭК.

“В первую очередь я хотел бы поздравить всех участников юбилейного 10 Форума с международным днем безопасного интернета. Безусловно, за последние 10 лет Форум значительно трансформировался. Это связано в первую очередь с тем, что каждый год и государство и отрасль актуализируют свою деятельность, направленную на предотвращение новых киберугроз. Я рад приветствовать всех участников и хотел бы еще раз подчеркнуть необходимость диалога между государством, отраслью и профильными организациями, с целью создания сильной коалиции противодействия киберпреступности”, – поприветствовал участников **Сергей Гребенников**, директор РОЦИТ.

Антонина Приезжева, заместитель руководителя Роскомнадзора обратила внимание на актуальные моменты:

“Темы, которые ежегодно обсуждаются в рамках мероприятия – актуальны всегда. Очевидно, что необходимо сократить проблемы между законодательством и профессиональной спецификой. Мы выявили основные источники киберпреступлений: хищение персональных данных, использование серых мобильных приложений, фишинг и другие. По нашему мнению, необходим комплексный подход к решению этих проблем. Особое внимание мы должны уделить субъектам персональных данных. Нами была разработана Стратегия информационно-публичной деятельности уполномоченного органа на период до 2020 года. В самом общем виде – это генеральная программа действий, правил. На систематической основе планируется проведение дня открытых дверей в образовательных учреждениях, направленных на повышение знаний в области защиты персональных данных. Традиционно мы не оставили без внимания детей. Мы продолжаем развивать информационные практические материалы для детей.

На официальной странице был размещен ролик “Береги свои персональные данные”. Федеральным собранием принят законопроект который дифференцирует ответственность за несоблюдение закона о персональных данных”.

Директор департамента государственной политики в области средств массовой информации Минкомсвязи России **Екатерина Ларина** обратила внимание собравшихся на необходимость внедрения культуры цифрового потребления:

“Самым необходимым фактором в кибербезопасности является осознанное использование сервисов, которые предоставляются и понимание пользователем всех тех рисков, которые есть. Мы начали работу над медиаграмотностью еще в прошлом составе Минкомсвязи. Нам видится медиаграмотность, как осознанное умение человека работать с информацией, которую он получает из самых разных источников. Естественных навыков у пользователей выработаться не успело, их необходимо воспитывать. Государство делает очень много для защиты пользователей в интернете. Это и законодательная база, и меры по защите персональных данных. Радует и осознанное отношение бизнеса к этой теме. Эти меры обеспечиваются государством и бизнесом. Но самое важное сегодня - просветительская работа о защите персональных данных в пользовательской среде.”

Андрей Воробьев, директор Координационного центра доменов.RU/.РФ говорил о трендах в области кибербезопасности:

“В 2016 году проявились несколько трендов в области информационной безопасности, которые хотелось бы отметить. Первый, это все большее участие государства в инициативах по регулированию интернета, активность профильных ведомств была очень высока. Второй – это большое внимание со стороны государственных организаций, общественности и бизнеса, уделяемое борьбе с противоправным контентом и повышению цифровой грамотности. Темы управления контентом все больше звучат в том числе на международных площадках, таких как ICANN. И третий очевидный тренд – это повышение роли саморегулирования и активное участие в этих процессах государственных органов. Так, в прошлом году Координационный центр подписал соглашение о присвоении статуса компетентных организаций Роскомнадзору и Центробанку, таким образом были созданы инструменты для оперативного противодействия мошенническим ресурсам”.

Презентация Рейтинга цифровой культуры

В рамках Cyber Security Forum компания Microsoft впервые презентовала рейтинг цифровой культуры. Согласно данным исследования Microsoft, примерно 75% россиян сталкивались хотя бы раз в жизни с интернет-рисками. По итогам исследования был составлен рейтинг стран по уровню цифровой культуры - Digital Civility Index (DCI). Россия заняла 12-е место среди 14 стран, принявших участие в опросе. РФ превышает

международные показатели по таким интернет-рискам, как агрессивное поведение в сети и риски нежелательных контактов.

В ходе исследования изучался негативный опыт взаимодействия пользователей в интернет-среде с точки зрения культуры и личной безопасности, а также последствия такого взаимодействия. Для измерения индекса DCI были выделены четыре основные категории рисков: поведенческие, риски нежелательных коммуникаций, сексуальные и репутационные. В опросе участвовали взрослые и подростки из 14 стран мира. Исследование показало, что интернет-угрозы широко распространены во всех странах – с ними сталкивались более 65% респондентов. Причем многие отметили реальные последствия после различных инцидентов в интернете. Наиболее распространённые среди них – потеря доверия, стресс и стремление пользователей к повышению конфиденциальности в сети. Опрос российской аудитории показал, что россияне, по сравнению с пользователями из других стран, больше других подвержены поведенческим рискам: оскорблениям в интернете (44% при среднем уровне в остальных странах в 14%), а также плохому обращению в сети (47% против 20%).

«Интернет-отрасль в нашей стране относительно молода. Еще десять лет назад интернет-пространство, его аудитория и ситуация в плане инфобезопасности были другими. Интернет-угрозы развиваются по мере технологического прогресса и роста аудитории сети. Главный и наиболее эффективный инструмент борьбы с ним – повышение уровня осведомленности пользователей, соблюдение правил сетевого этикета, знания о том, как предостеречь себя от рисков в интернете и как реагировать на них. Задача индустрии и всех нас заключается в том, чтобы предоставить пользователям эти знания, повышая интернет-грамотность. Это поможет упростить жизнь и обезопасить себя в интернете, а безопасность в виртуальной среде оказывает прямое влияние на нашу повседневную безопасность в реальной жизни», – отметил директор Ассоциации электронных коммуникаций, член правления Регионального общественного центра интернет-технологий **Сергей Плуготаренко**.

«Microsoft серьезно относится к защите информации своих пользователей и разрабатывает безопасные онлайн-сервисы и продукты, поддерживает такие международные инициативы, как День безопасного интернета, – говорит **Ульяна Зинина**, директор по корпоративным вопросам компании Microsoft в России. – Для снижения вероятности рисков в сети Microsoft призывает заинтересованные стороны объединить усилия, а пользователей следовать ключевым рекомендациям: не публиковать и не раскрывать информацию личного характера о себе на общедоступных ресурсах, относиться с уважением к другим пользователям, культурным различиям и другим точкам зрения. В случае несогласия стоит осознанно подходить к ответным действиям, избегать навешивания ярлыков и не переходить на личности, оказывать поддержку пострадавшим от негативного взаимодействия в интернете».

В заключении официального открытия Форума главный аналитик РОЦИТ **Урван Парфентьев** отметил, что цифровые технологии глубоко проникли в жизнь рядового пользователя и сегодня мы должны заботиться в первую очередь о повышении цифровой грамотности населения, о повышении этики взаимодействия всех субъектов информационных взаимоотношений. Урван также подчеркнул, что такая работа ведется и на международном уровне.

УЗНАЙ ЧТО В ОБЛАКЕ?

Источник: http://www.liga.net/projects/cloud_storage/

«Что, черт возьми, это такое – облачные вычисления?» – сказал Гендиректор *CEO Oracle Ларри Эллисон* на встрече с финансовыми аналитиками в сентябре 2008 года. «Может быть, я идиот, но я вообще ничего не понимаю, о чем это говорят люди», – добавил он, отзываясь о свежих статьях в прессе. *Эллисон* тогда много шутил над прочитанными фразами, что cloud computing – это компьютеры, которые находятся где-то там. «Люди, которые написали эту чушь, – они тоже где-то там», – продолжал он.

Гендиректор тогда вряд ли мог даже догадываться, что продажи Oracle Cloud Computing через десять лет будут составлять $5 млрд в год. Мировой облачный рынок превратился в огромную экосистему с заоблачными сделками. К примеру, мессенджер Snapchat недавно сообщил, что в последующие пять лет потратит $1 млрд на облако от Amazon. Буквально перед этим компания заявила, что в течение этого же промежутка времени она вложит $2 млрд в сервисы на облаке Google.

"Облака стали новой нормой, так как компании любого размера теперь по умолчанию развертывают новые приложения в облаке и стремятся перенести туда как можно больше своих приложений в самые короткие сроки. Предприятия больше не спрашивают, "стоит ли?". Они спрашивают "как быстро мы можем это сделать?" и "что мы будем переносить в первую очередь?" – рассказал Liga.net *архитектор решений Amazon Web Services Денис Баталов*.

ЗМІСТ