SafeNet: защита в облаках

С сентября 2012 г. по апрель 2013 г. компанией SafeNet были анонсированы три решения: StorageSecure – совместная разработка с NetApp, ProtectV и Crypto Hypervisor. Таким образом, SafeNet представила законченное семейство решений для защиты сервисов (и их данных) и виртуальных инфраструктур на основе аппаратных средствах криптографии, в значительной степени упростив и снизив стоимость управления ключами шифрования с клиентской стороны в составе гибридных облаков и распределенных ИТ-сред.

Сергей Кузнецов – директор SafeNet в России и СНГ.

Введение

До самого последнего времени все усилия по организации безопасности были сконцентрированы на защите периметра и ожиданиях, что постоянно развивающиеся средства обороны (защиты) смогут опережать концептуально и технологически средства атакующих. К сожалению, за последними остается "поле битвы", и список громких побед хакеров над современными методами защиты уже вошел в аналы истории: Zappos – 24 млн записей, Global Payments – 1,5 млн, Yahoo – 800 тыс., LinkedIn – 1,5 млн, и этот список можно продолжить.

Вероятность таких утечек до недавнего времени возрастала по мере миграции от датацентров с охраняемым периметром к публичным облакам и распределенным ИТ-инфраструктурам с возможностью доступа к корпоративным данным с любого устройства, из любого места, в любое время.

В целях снижения подобных рисков с 2010 г. во всех развитых странах были приняты регламентирующие документы, основная суть которых – необходимость шифрования данных на всех стадиях: от передачи до обработки. Шифрование данных в облаке было признано в качестве одного из основных защитных механизмов, снижающих риски компрометации данных, рекомендованных Cloud Security Alliance. Помимо этого, были повышены требования и к защите самих виртуальных инфраструктур.

Многие компании уже сталкивались в быту с простыми алгоритмами шифрования, которые были недостаточно надежны и, возможно, даже послужили причиной потери информации, которую пользователи не смогли корректно извлечь. Причин могло быть много: программные сбои, забытые пароли, некорректно написанное свободно распространяемое программное обеспечение. В корпоративных системах безопасности подходы кардинально отличаются. Единственные решения, которым доверяют, – основаны на "железе". Именно аппаратному обеспечению профессионалы безопасности готовы доверять хранение ключей шифрования. Это понятно. Не так важно, где находятся ваши зашифрованные данные, если ключ хранится в надежном месте, имеет резервную копию и может быть использован только его владельцем. Хорошими примерами аппаратных устройств хранения ключей могут служить в простых случаях – токены, когда есть задача шифровать, например, диски на персональном компьютере, в сложных – Аппаратные Модули Безопасности (Hardware Security Modules, HSM) или еще более мощные устройства хранения и управления жизненным циклом ключей – новые высокопроизводительные платформы KeySecure. Ведь именно аппаратные средства хранения ключей, которые в дальнейшем используются для шифрования данных, часто являются сердцем системы.

Разобравшись с ключами, рассмотрим аспекты шифрования данных. В свете того, что количество данных в мире более чем удваивается каждый год, а практически любая компания имеет обыкновение собирать информацию и постоянно ее накапливать, то задача шифрования принимает серьезный масштаб. В этом случае использование традиционно предлагаемых программных решений, имеющихся в широком наличии у производителей баз данных, имеет ряд серьезных недостатков. Они связаны с производительностью систем и дороговизной, поскольку добавление такой ресурсозатратной операции, как шифрование, да еще в режиме реального времени, потребует серьезного увеличения серверных ресурсов, а в ряде случаев – и пересмотра архитектуры. Стоимость самого компонента программного обеспечения также стоит принять во внимание во избежание неожиданностей.

Суть подхода компании SafeNet к защите данных строится на использовании независимой аппаратной платформы, высокопроизводительной, с хорошей масштабируемостью и возможностью полного резервирования. Последнее – один из наиболее важных аспектов всех систем шифрования масштаба предприятия. Очень важным является прозрачность системы для конечных пользователей, сотрудников ИТ и ИБ, что позволит избежать дополнительных расходов по перестроению архитектуры информационных систем и моделей использования их конечными пользователями.

StorageSecure – защита совместно используемых файловых хранилищ

"В результате стремительного роста объемов цифрового контента и неструктурированных данных растет и количество пользователей, внедряющих у себя масштабируемые файловые сетевые системы хранения данных. Консолидация корпоративных данных, в том числе конфиденциальной информации, и перенос их в крупные централизованные репозитарии приводит к появлению целого ряда проблем и угроз безопасности, связанных с соблюдением нормативно-правовых требований. Многопользовательские NAS-окружения предполагают увеличение числа пользователей и администраторов СХД, имеющих права доступа к одному и тому же окружению хранения данных. Для предотвращения несанкционированного доступа и недопущения использования конфиденциальных данных, а также для целей эффективного аудита, пользователям необходимо внедрять новые методы защиты своих данных", – отмечает Сид Дишпэнд *(Sid Deshpande)*, аналитик Gartner.

StorageSecure – первое из решений для защиты файловых сетевых хранилищ (NAS) в облачных средах в условиях мультиаренды с полным управлением ключами шифрования с клиентской стороны. Система StorageSecure была разработана в сотрудничестве с NetApp.

StorageSecure строится на базе апплайнса, который выпускается в двух модификациях – S220 (с 1GbE интерфейсом для подключения) и S280 (с 10GbE интерфейсом). Устройство устанавливается в сети между клиентами и серверами, связывая их по шифрованному каналу. При этом не требуется установка какого-либо управляющего сервера или ПО – "все включено". Для обеспечения бОльшей доступности устройства могут конфигурироваться в кластер.

Среди основных преимуществ решения StorageSecure следующие:

– *защита данных на основе политик безопасности*. Гранулярное шифрование данных, передаваемых с помощью файловых систем CIFS (Common Internet File System) и NFS (Network File Service), на уровне каталогов, с разделением данных, хранящихся в окружениях NAS для общего доступа, позволяет гарантировать, что данные пользователей будут полностью изолированы и защищены от несанкционированного доступа со стороны других пользователей или администраторов.

Впервые в отрасли был представлен дополнительный уровень защиты от неблагонадежных администраторов. Кроме того, заказчики получают возможность эффективного уничтожения данных по мере необходимости;

– *расширенные средства для управления данными (Data Governance)*. Устройство StorageSecure отвечает требованиям стандарта безопасности FIPS 140-2 Level 3 и представляет собой устойчивое к взлому сетевое устройство с гарантированным аудитом и централизованным управлением политиками безопасности, которое позволяет хранить ключи шифрования и управлять ими в полностью защищенном режиме. Все это дает возможность вести максимально полный аудит событий доступа к конфиденциальной информации, хранящейся в сетевых системах хранения данных;

– *защита инвестиций*. Устройство StorageSecure интегрируется в существующие ИТ архитектуры, может использовать существующие политики безопасности и средства клиентской аутентификации Active Directory, Lightweight Directory Access Protocol (LDAP) или Network Information Service (NIS), и поддерживает работу любых NAS устройств и файловых серверов на базе протоколов CIFS и NFS. С 4-го кв. 2012 г. стал также поддерживаться протокол iSCSI;

– *кросс-платформенное управление ключами*. Являясь частью портфеля решений SafeNet для защиты данных, устройство StorageSecure интегрируется с корпоративным решением SafeNet для управления ключами – KeySecure™. KeySecure дает возможность сотрудникам служб информационной безопасности централизованно управлять ключами шифрования для всех платформ шифрования, использующихся на предприятии. В то же время это решение позволяет упростить процедуру администрирования ключей и политик. Построенное на базе протокола KMIP (стандартного отраслевого протокола для управления ключами) KeySecure обеспечивает возможность управлять ключами для устройства StorageSecure и для самых разнообразных решений для шифрования СХД, в том числе для систем шифрования в сетях хранения данных (SAN). В числе прочего решение позволяет управлять ключами к коммутаторам шифрования Brocade encryption switch (BES), к самошифрующимся накопителям (self-encrypted drives, SED), используемым во многих современных сетях хранения данных и сетевых хранилищах (например, в NetApp NSE), а также к самошифрующимся ленточным накопителям для резервного копирования данных.

ProtectV – полнофункциональное решение для защиты данных и виртуальных инфраструктур в облачных окружениях

Решение ProtectV стало доступно 11 сентября 2012 г. В отличие от StorageSecure, оно уже обеспечивает не только защиту данных, но и защиту всей виртуальной инфраструктуры, развертываемой в виртуализируемом публичном облачном окружении (рис. 1).

По мере того, как все бОльший объем данных переносится в частное или публичное облако, увеличивается и количество привилегированных пользователей, имеющих доступ к корпоративным данным. Вместе с этим увеличивается риск создания копий виртуальных машин без ведома владельцев, повышается вероятность хищения временных файлов, при этом корпоративные данные становятся более уязвимыми и подверженными компрометации. Для решения проблем, возникающих с обеспечением безопасности данных, а также для контроля и управления данными в облачном окружении служит решение для шифрования информации ProtectV, которое прошло сертификацию VMware Ready™. Решение SafeNet ProtectV совместимо с инфраструктурами VMware vShield™ и VMware vCenter™. Кроме того, решение SafeNet ProtectV поможет пользователям сервисов Amazon Web Services (Amazon Web Services EC2, Amazon VPC) защитить свои данные, размещенные в облаке.

Решение ProtectV обеспечивает такую же высокую безопасность виртуальных машин и виртуальных разделов хранения данных, как если бы это были физические серверы и физические системы хранения данных, размещенные в надежном, защищенном окружении на территории заказчика. При этом заказчики получают все преимущества высокой гибкости, устойчивости и экономии затрат за счет превращения своего виртуального центра обработки данных или облака в надежное, защищенное окружение с возможностью управления данными, контроля над ними и с высоким уровнем безопасности.

С помощью ProtectV заказчики смогут защитить важные данные на протяжении всего их жизненного цикла: от момента подготовки и инициализации (provisioning) до уничтожения.

Среди основных возможностей решения ProtectV следующие:

– *полная защита виртуальных машин и изоляция данных*. Решение SafeNet ProtectV позволяет осуществлять гранулярное и полное шифрование всей виртуальной машины, поддерживает предстартовую аутентификацию и размещение отправной точки доверия (root of trust) на оборудовании на стороне заказчика, что обеспечивает комплексную защиту на всем протяжении жизненного цикла информации. ProtectV позволяет запускать системы, даже в совместном (co-mingled) или многопользовательском окружениях, как если бы они находились в Вашем собственном частном центре обработки данных. Теперь сотрудники службы безопасности смогут должным образом изолировать конфиденциальные или иные важные данные и сохранять полный контроль над данными на всем протяжении их жизненного цикла;

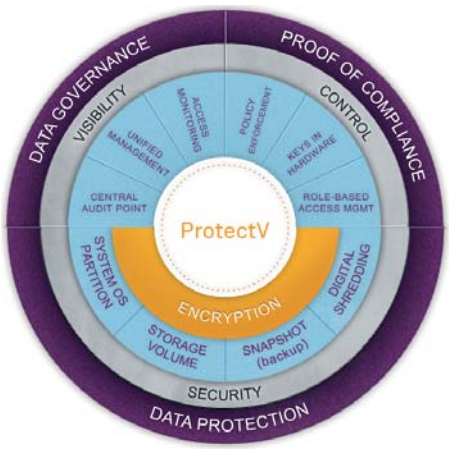


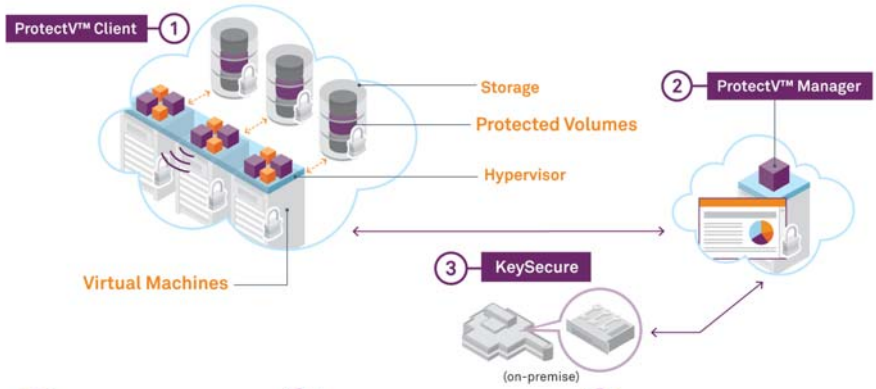
Рис. 1. Решение ProtectV обеспечивает полную защиту всей пользовательской виртуальной инфраструктуры (включая данные и сервисы данных), а также поддерживает требования регуляторов.

– *защита от недобросовестных администраторов*. Все виртуальные машины и соответствующие им разделы для хранения данных шифруются – сюда относятся копии виртуальных машин, их конфигурации (snapshot) и резервные копии на всех узлах и площадках аварийного восстановления. Таким образом, привилегированные пользователи и администраторы, в чьих руках может находиться контроль над инфраструктурой виртуализации, не смогут получить доступ к зашифрованным виртуальным машинам;

– *выполнение требований законодательных нормативных актов*. Решение ProtectV обеспечивает механизм фиксируемого контроля (undisputed control) с подтверждением операций по управлению данными через журналы аудита. ProtectV позволяет организациям добиться надлежащего контроля и обеспечить надежное управление аудитом (audit control) вне зависимости от того, где размещаются или хранятся данные, соблюдая при этом требования законодательных нормативных актов, включая PCI DSS, HIPAA и HITECH;

– *управление данными (Data Governance) и прозрачность*. Решение ProtectV позволяет получить наглядное представление о безопасности внутри облака за счет централизованной реализации политик шифрования и использования единой точки аудита (audit point). SafeNet обеспечивает высоконадежное и безопасное окружение для управления ключами с фиксируемым контролем доступа к данным и ключам. Таким образом, предприятия и их аудиторы, проверяющие инфраструктуру на соответствие требованиям законодательных актов, гарантированно получают полный контроль над ключами к данным, а также журналы доступа к ним, что позволяет достичь необходимой прозрачности;

– *кроссплатформенное управление ключами*. Даже самое надежное шифрование не имеет смысла без грамотного управления ключами. В рамках портфеля решений SafeNet для защиты данных, система SafeNet ProtectV интегрируется с корпоративным решением SafeNet для управления ключами



1 **ProtectV Client** устанавливается на защищаемую ВМ. С помощью него выбираются серверы и тома, которые подлежат шифрованию и управлению на основе создаваемых политик.

2 **ProtectV Manager** представляет виртуальную машину, которая работает как AWS AMI или как VM в VMware окружениях. Конфигурируя ProtectV Manager, можно создавать пользователей и устанавливать для них права доступа к данным.

3 **KeySecure** – опционная компонента для пользователей, которым требуется обеспечение более высокого уровня безопасности. KeySecure позволяет обеспечить управление жизненным циклом всех типов ключей для частных ипубличных облаков.

Рис. 2. Решение ProtectV имеет три ключевые компоненты: ProtectV Client, ProtectV Manager и KeySecure.

– KeySecure™. KeySecure позволяет сотрудникам служб информационной безопасности централизованно управлять ключами шифрования для всех платформ шифрования, использующихся на предприятии. В то же время, это решение позволяет упростить процедуру администрирования ключей и политик.

Решение ProtectV имеет три ключевые компоненты (рис. 2): ProtectV Client, ProtectV Manager и KeySecure. ProtectV Client устанавливается на каждую ВМ заказчика, которая должна защищаться. Эта компонента шифрует каждый бит, записываемый на диск. Управление шифрованием осуществляется на основе создаваемых политик. В дополнение она предлагает pre-launch-аутентификацию для защиты операционной системы от неавторизованного доступа, когда система инициируется.

ProtectV Manager выполняется на защищенной виртуальной машине, которая работает как AWS AMI или как VM в VMware окружениях. ProtectV Manager представляет централизованную платформу для управления политиками, администрированием и аудитом. Конфигурируя ProtectV Manager, можно создавать пользователей и устанавливать для них права доступа к данным.

KeySecure – обязательная компонента, разворачиваемая на дополнительной аппаратной платформе. Она предназначена для пользователей, которым требуется обеспечение более высокого уровня безопасности. KeySecure позволяет обеспечить управление жизненным циклом всех типов ключей для частных и публичных облаков.

Crypto Hypervisor: сервисы шифрования по запросу в облачной модели эксплуатации ИТ-инфраструктуры

В конце апреля 2013 г. SafeNet анонсировала ограниченную доступность решения Crypto Hypervisor, призванного упростить и снизить стоимость управления ключами шифрования до 95%. Архитектура решения представлена на рис. 3.

Как и традиционный гипервизор, Crypto Hypervisor позволяет астрагировать аппаратные модули безопасности от конечных пользователей.

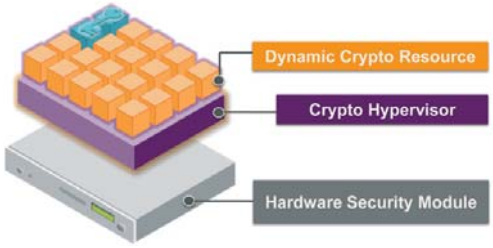


Рис. 3. Архитектура решения Crypto Hypervisor.

Основными компанентами Crypto Hypervisor являются:

– Crypto Command Center – программное обеспечение, автоматизирующее предоставление криптографических ресурсов пользователям, посредством абстракции HSM;

– аппаратный модуль безопасности SafeNet Luna SA 5 – высоконадежная, проверенная временем, платформа реализующая аппаратное хранение ключей шифрования.

NIST[1] Cloud Definition of Essential Characteristics	Legacy HSMs
On-Demand Self-Service	No
Rapid Elasticity	No
Measured Service	Some
Broad Network Access	Yes
Resource Pooling	Some
Multi-Tenancy[2]	No

NIST[1] Cloud Definition of Essential Characteristics	Crypto Hypervisor
On-Demand Self-Service	Yes
Rapid Elasticity	Yes
Measured Service	Yes
Broad Network Access	Yes
Resource Pooling	Yes
Multi-Tenancy[2]	Yes

(1) National Institute of Standards and Technology
(2) Multi-Tenancy или мультиаренда – основная характеристика добавляемая Cloud Security Alliance

Рис. 4. Решение Crypto Hypervisor расширяет возможности HSM-модулей в соответствии с требованиями облачной модели.

С помощью решения SafeNet Crypto Hypervisor ИТ-подразделения и поставщики услуг смогут по мере необходимости осуществлять доставку сервисов хранения адаптивных ключей шифрования (elastic key vaulting) и сервисов шифрования для защиты данных в физическом, виртуальном и облачном окружениях не за дни, как было раньше, а за минуты. Сервисы высоконадежного шифрования, реализованные в системе, полностью отвечают требованиям, предъявляемым к облачным моделям (рис. 4). Система обеспечивает все преимущества виртуализации с точки зрения оптимизации затрат и повышения уровня инноваций, без ущерба для безопасности и с полным соблюдением установленных требований. При этом сохраняется полный централизованный контроль за доставкой сервисов шифрования, таких как безопасное хранение ключей. Пользователь получает полный контроль над своими сервисами шифрования и может быть уверенным, что его ключи шифрования не доступны для других пользователей или для администраторов системы.

"Хотя шифрование все чаще встречается в ИТ-практике компаний, безопасность данных полностью зависит от безопасности ключей, с помощью которых эти данные защищены, – говорит Кристиан Кристиансен (Christian A. Christiansen), вице-президент IDC по продуктам и услугам безопасности в IDC. – Хранение ключей на специализированном аппаратном обеспечении, например на аппаратных модулях безопасности, является наиболее предпочтительной передовой практикой. Однако до сих пор аппаратные решения шифрования не отличались достаточной динамичностью и гибкостью, которые необходимы в виртуализированных и облачных окружениях. Развертывание виртуального приложения, требующего шифрования, подписанных цифровых сертификатов или других функций PKI, зачастую увеличивало сроки реализации проекта на несколько дней, а то и недель".

Решение SafeNet Crypto Hypervisor позволяет справиться с этими задачи благодаря расширению и виртуализации аппаратного модуля безопасности SafeNet Luna SA 5 Hardware Security Module (HSM), за счет чего он может использоваться в ИТ-моделях с виртуальным и облачным окружениями. Администраторы криптографических систем могут централизованно управлять и конфигурировать решение Crypto Hypervisor через центр управления SafeNet Crypto Command Center. При этом администраторы могут создавать каталоги сервисов, доступных в Crypto Hypervisor, а пользователи могут через веб-портал просматривать персонализированные каталоги тех сервисов, для развертывания которых у них имеются права. Эти пользователи могут использовать необходимые им сервисы в режиме по требованию на общем физи-

ческом оборудовании. Этот процесс позволяет сократить сроки развертывания новых сервисов с нескольких дней до нескольких минут.

Основные преимущества решения SafeNet Crypto Hypervisor:

– *криптографические сервисы, совместимые с облачным окружением*. Созданное для облачной модели решение Crypto Hypervisor позволяет организациям консолидировать нагрузку по осуществлению шифрования, устранить, так называемые "островки шифрования" и обеспечить более безопасную и эффективную работу. Организации могут задействовать всего лишь пять процентов от сегодняшнего количества единиц используемого аппаратного обеспечения для осуществления того же объема услуг шифрования;

– *снижение общей стоимости*. При первичной инициализации каталог сервисов шифрования может определяться центральной группой администраторов. После этого различные пользователи из различных организаций могут заказывать эти высоконадежные сервисы защищенного хранения ключей по мере необходимости непосредственно из этого онлайн-каталога. В результате новые сервисы, для доставки которых обычно требовалось несколько дней или даже недель, теперь могут быть реализованы за несколько минут, без вмешательства центральной ИТ-организации;

– *централизованное управление*. Центр управления Crypto Command Center позволяет работать с сотнями независимых виртуализированных аппаратных модулей HSM. При этом для всех функций реализован аудит с фиксированием попыток несанкционированного доступа и ведением журналов доступа с цифровой подписью. Подобное централизованное управление и журналирование позволят заказчикам создать центры передовых технологий в области шифрования и оптимизировать процессы аудита;

– *наиболее безопасная технология хранения ключей*. Решение Crypto Hypervisor представляет собой виртуализированную версию надежных и проверенных аппаратных модулей безопасности SafeNet Luna HSMs, которые сегодня ежедневно используются для защиты финансовых транзакций с совокупным дневным оборотом более 1 триллиона долларов; обеспечивают доступность на уровне 99,999% и которым доверяют предприятия и правительства по всему миру.

Решение SafeNet Crypto Hypervisor запускается на аппаратной платформе SafeNet Luna SA 5 HSM, которая уже в продаже. Пакет Crypto Command Center доступен для предварительного заказа. ПО Luna 5.2 HSM и решение Crypto Command Center доступны в ограниченном количестве для ряда покупателей.

Платформа Luna SA доступна в двух модификациях: Luna 7000 и Luna SA 1700. Luna SA 7000 – высокопроизводительная модель, поддерживающая широкий ряд алгоритмов включающих ECC, RSA и

Табл. 1. Производительность (транзакций/сек) моделей Luna SA для различных алгоритмов

Алгоритм	Модель	
	Luna SA 1700	Luna SA 7000
RSA-1024	1700	7000
RSA-2048	350	1200
ECC P256	500	1000
ECIES	200	300
AES-GCM	3700	3700

симметричные транзакции. Luna SA 7000 имеет сдвоенные hot-swappable источники питания, гарантирующие отсутствие какого-либо времени простоя. Низкопроизводительная модель Luna 1700 включает один источник питания и способна поддерживать 1700 RSA 1024-bit транзакций в секунду (табл. 1).

Заключение

Все анонсированные в последнее время решения будут доступны в России и СНГ уже в ближайшее время – во второй половине 2013 г. – с возможностью их тестирования на стендах.

В целом, решения StorageSecure, ProtectV, Crypto Hypervisor, KeySecure, а также сервис аутентификации – SafeNet Authentication Service позволяют полностью решить задачу централизованного управления ключами шифрования (в интеграции с криптографическими компонентами от других производителей – NetApp Self Encryption, Brocade Encryption Switch, Hitachi, Quantum и др.) в облачных и распределенных ИТ-инфраструктурах, минимизируя сложность управлениия и стоимость эксплуатации/развертывания.

Сергей Кузнецов,
SafeNet в России и СНГ.

"ИнфоБЕРЕГ–2013"

Май 2013 г. – Открыта регистрация на всероссийскую конференцию "Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ–2013", которая пройдет с 10 по 15 сентября в Лазаревском, SPA-отеле "Прометей-клуб".

В конференции традиционно примут участие представители федеральных органов государственной власти, законодательных, контролирующих и регулирующих структур Российской Федерации. Конференция пройдет при поддержке Министерства энергетики РФ.

Основные темы конференции:

– безопасность ТЭК (ФЗ-№ 256, защита АСУ ТП КВО ТЭК);
– безопасность Сочи–2014;
– противодействие кибератакам на информационные ресурсы;
– электронная подпись;
– открытое ПО и кибербезопасность;
– ИБ в банковской сфере в свете закона о НПС;
– защита информации от внутренних угроз;
– безопасность облачных и мобилных вычислений.

В этом году особое внимание уделено научной секции с возможностью публикации материалов в журнале, аккредитованном Высшей Аттестационной Комиссией.

Регистрация на сайте: *http://vipforum.ru/registration.html.*

NetApp Connect: поддержка BYOD

Май 2013 г. – Компания NetApp объявила о выходе нового решения NetApp® Connect, которое призвано обеспечить безопасный, удобный и быстрый доступ с мобильных устройств к данным, хранящимся в СХД NetApp. Решение, созданное на базе технологии, приобретенной NetApp у компании ionGrid, легко интегрируется в среды NetApp без необходимости в сложной настройке сети VPN или в прохождении дополнительной аутентификации. Кроме того, все данные остаются в локальной системе хранения, при этом обеспечиваются легкость доступа для пользователей и простота управления для организации.

NetApp Connect дополняет быстро растущую линейку мощных мобильных решений, разработанных NetApp совместно с партнерами, в которую также входят продукты Citrix ShareFile™ и программный пакет VMware® Horizon™, позволяя NetApp предлагать корпоративным заказчикам еще больше новых возможностей. Разработанные совместно с партнерами решения, интегрированные с функциями управления данными СХД NetApp (или архитектурой clustered Data ONTAP ®), обеспечивают эффективное и безопасное сотрудничество, обмен файлами и мобильный доступ к данным.

Приложение NetApp Connect функционирует так же, как и любое другое приложение для iPhone или iPad. Однако оно является высокоуправляемым решением и создает на мобильном устройстве безопасный контейнер, позволяя хранить данные под постоянным контролем. Он также дает возможность руководителям ИТ-отделов поднять управление корпоративными данными и доступом пользователей к ним на новый уровень, что обеспечивает соблюдение существующих правил и политик и вселяет уверенность, что запрашиваемая информация попадет на нужное устройство к нужному сотруднику в нужное время. NetApp Connect не требует сложной установки, а также копирования или преобразования данных, поэтому установка приложения займет минимум времени и обеспечит надежную защиту данных компании. Теперь данные остаются под надежной защитой корпоративного брандмауэра и не копируются в облачную среду, что обеспечивает бескомпромиссную безопасность доступа к корпоративным данным и надежность управления ИТ-инфраструктурой. При этом данные могут находиться в домашних каталогах, на Microsoft® SharePoint® или в приложениях внутренних сетей. Это позволяет интегрировать мобильные устройства в рабочие процессы и повысить производительность сотрудников компании.

Приложение NetApp Connect уже доступно на Apple App Store и в скором времени будет оптимизировано для работы с другими мобильными устройствами.