УДК 004.047

О.В.Копейка

АРХИТЕКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ ИТ-ИНФРАСТРУКТУРЫ В ДАТА-ЦЕНТРАХ

В статье рассмотрены варианты формирования архитектуры системы безопасности в современных дата-центрах. Архитектура системы безопасности обеспечивает необходимый уровень защиты ИТ-активов корпорации путем описания подходов по организации и формированию требований к персоналу, процессам и технологиям. Задача безопасности ИТ заключается в обеспечении защиты ценной информации и обеспечение ее доступности авторизованным пользователям.

Ключевые слова: **д**ата-центр, архитектура системы безопасности, доступность, защита и управление цифровыми данными .

Введение и постановка задачи

В ближайшее десятилетие глубокое влияние на бизнес будут иметь «облачные» технологии. Сегодня ими пользуются 46 процентов опрошенных компаний, а те предприятия, которые еще этого не сделали , планируют перейти от традиционных центров обработки данных к облачным вычислениям в течение ближайших пяти лет. К 2020 году информационно - технологические вычисления почти полностью перейдут в облако, а граница между корпоративными и персональными вычислениями окажется сильно размытым.

При этом следует отметить, что рынок услуг дата-центов в странах СНГ начал формироваться в 2000 году и до сих пор находится в стадии становления. Отсутствует нормативное регулирование рынка, нет четкой градации оказываемых услуг, фактически отсутствует конкуренция. В этом его основное отличие от рынка дата-центров в США и Европе, который начал формироваться в 1990-х годах (на 10 лет раньше) и в настоящее время развит гораздо лучше и хорошо регламентирован и стандартизован. Тем не менее, даже в США наблюдается недостаток предложения на рынке дата-центров, в период кризиса некоторые проекты по строительству новых дата-центров будут заморожены и прогнозируемого расширения площадей не произойдет.

В последнее время основным фактором перехода к централизованному использованию ИТ ресурсов является распростанение «облачных» технологий. При этом, перед компаниями возникает перспектива не только переноса серверов в дата-центры, а и модернизации всей ИТ инфраструктуры вцелом.

В данной статье будем рассматривать развитие системной архитектуры ИТ инфраструктуры корпорации.

Целью данных исследований является выработка стратегии развития системной архитектуры ИТ инфраструктуры корпорации на основе применения передовых методологий и концепций ведущих производителей аппаратного и програмного обеспечения (HP, SUN, EMC, CISCO, Microsoft, ORACLE, Veritas).

Основной задачей при этом является разработка архитектур ИТ инфраструктуры, которые определяют фундаментальные принципы построения ИТ сервисов и их взаимосвязь. Также на базе архитектур формируются требования к созданию ИТ сервисов. Мы выделяем следующие архитектуры: управления; хранения данных; приложений; сетевая; безопасности.

Одной из самых важных архитектур является архитектура системы безопасности.

Основная часть

Задача безопасности ИТ заключается в обеспечении защиты ценной информации и обеспечение ее доступности авторизованным пользователям. Невыполнение задачи безопасности может привести к:

1. Удалению или изменению информации.
2. Краже информации или сервиса.
3. Нарушению бизнес операций.

4. Нанесению ущерба репутации компании.

Архитектура безопасности обеспечивает необходимый уровень защиты ИТ-активов корпорации путем описания подходов по организации и формированию требований к персоналу, процессам и технологиям.

Корпоративная инфраструктура должна соответствовать стандарту British Standard 7799 и его развитию International Organization for Standardization (ISO) Standard 17799. Политики корпорации, разработанные в соответствии с данными стандартами могут предоставить необходимый уровень требований к персоналу, процессам и технологиям для обеспечения корректного использования ИТ активов авторизованными пользователями.

Архитектура безопасности разрабатывается на базе трех компонентов:

1. Процесс дисциплины управления рисками.
2. Зонирование сети.
3. Эшелонная защита.

ИТ- активы

ИТ-активы – ресурсы имеющие ценность для работы корпорации. ИТ-активы включают, но не ограничиваются ими, два компонента – данные (информация, информационный сервис) и уровни.

Архитектура безопасности обеспечивает для данных (или информации) защиту:

1. Конфеденциальности. Защита он несанкционированного доступа и использования информации.

2. Целостности. Защита от неавторизованой, неумышленной модификации или повреждения информации.

3. Доступности. Корпорация должна предоставлять информацию или сервисы вовремя, в пределах временных рамок определенных клиентом.

Уровни представляют собой набор узлов или устройств, которые имеют однотипную функциональность и могут рассматриваться как один логический компонент.

Персонал

Основные принципы безопасности, затрагивающие персонал:

1. Создаются и используютсяполитики безопасности.
2. Персонал имеет достаточную квалификацию для защити ИТ-активов с которыми он работает.
3. Персонал знает о политиках и их изменениях.
4. Существуют механизмы аутентификации пользователей и авторизации их действий с данными.
5. Администраторы и комиссии имеют возможность аудита действий и контроля выполнения политик.

Процесс дисциплины управления рисками

Архитектура безопасности включает в себя один процесс, базирующий на дисциплине управления рисками безопасности - Security Risk Management Discipline (SRMD). Процесс состоит из четырех последовательных шагов:

1. Определение и оценка ИТ-активов.
2. Идентификация рисков безопасности.
3. Анализ рисков.
4. Разработка и уменьшение рисков.

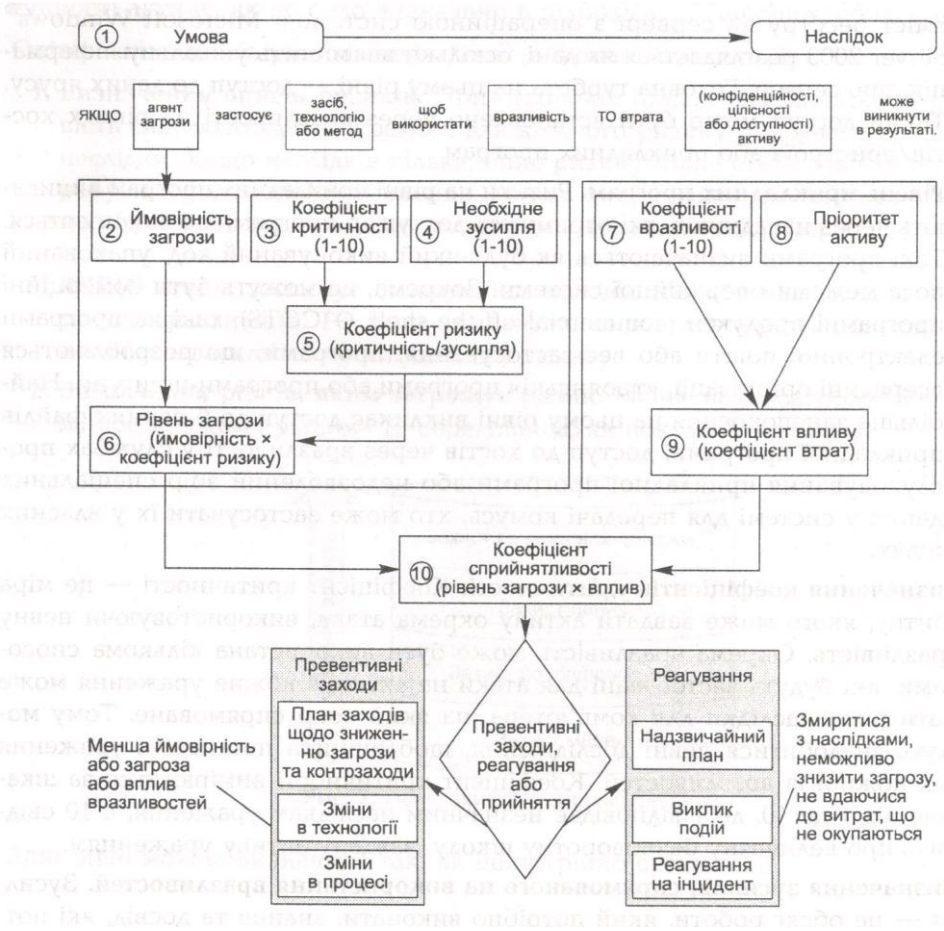

Рис. 1 Методика управления рисками

Шаг 1. Определение и оценка ИТ- активов

Определение активов включает в себя классификацию данных, используемых в корпорации: конфигурационная информация маршрутизатора, приказы и внутренние распоряжения, базы данных с информацией о клиентах, документы уровня коммерческой и государственной тайны.

Кроме информации при определении выделяются уровни (логические группы однотипных устройств и узлов).

Оценка активов включает анализ:

1. Физической стоимости компонента ИТ инфраструктуры:

а) стоимость аппаратной части;

б) стоимость программной части;

в) стоимость поддержки, эксплуатации;

г) стоимость замены;

1. Бизнес стоимости – стоимость актива для выполнения миссии корпорации.
2. Непрямой стоимости.
3. Конкурентной стоимости – стоимость актива с точки зрения перехода к конкурирующей организации.

После определения и оценки необходимо приоритезировать ИТ-активы. Каждому активу присваивается значения AP (asset priority) в соответствии с которым активы упорядочиваются. Факторы, которые влияют на формирование упорядоченного линейного списка:

1. Стоимость актива.
2. Цена его создания.

3. Цена его защиты.
4. Цена его поддержки.
5. Цена его восстановления.
6. Стоимость актива для конкурентов.

Результатом первого шага процесса будет четыре документа:
1. Список классифицированных данных.
2. Список классифицированных уровней.
3. Список оцененных активов.
4. Список приоритезированых активов.

Шаг 2. Идентификация рисков безопасности

Идентификация рисков безопасности опирается на следующие термины:

Угроза - потенциальная опасность, человек, вещь или событие, которое угрожает безопасности актива.

Агент угрозы - форма носителя угрозы – преступник, хакер, пожар, землетрясение.

Уязвимость - аппаратная, программная, процедурная точка удобная для осуществления атаки агентом угрозы.

Метод атаки (exploit).

Риск - значение функции, связывающей актив, угрозу, уязвимость и метод атаки.

Идентификация рисков включает в себя:

1**. Анализ угроз**. Кто угрожает каждому из активов?

2**. Оценка уязвимостей**. Какие у активов есть уязвимости? Какие атаки имели место в мировой практике? Какие последствия этих атак?

3**. Создание списка рисков:**

а). Определение риска в формате «ЕСЛИ агент угрозы посредством метода или инструмента воздействует на уязвимость, ТОГДА потеря (конфиденциальности, целостности, доступности) актива может отразиться в результате».

б).Определение уровня приложения риска: уровень данных, приложения, узла, сети, физического доступа.

в). Определение критических факторов (CF) – уровня разрушения актива в случае успешной атаки.

г). Определения уровня стоимости атаки (E) - количества знаний, опыта, работы требуемой для выполнения атаки.

д). Определение уровня подверженности данному типу атаки (VF) – фактор, который позволяет связывать различные активы с одним типом атаки.

4. **Оценка рисков** – процесс количественной оценки рисков.

Результатом второго шага процесса будут три документа:
1. Список угроз и методов их осуществления.
2. Список уязвимостей.
3. Таблица рисков.

Шаг 3. Анализ рисков

На третьем этапе для каждого из выделенных рисков определяются следующие параметры:
1. Вероятность риска.
2. Результат риска (последствия).

В результате анализа всех полученных количественных характеристик рисков создается «Основной список приоритезированных рисков».

Шаг 4. Разработка и уменьшение рисков

В разработку берутся только риски из документа «Основной список приоритезированных рисков». Для каждого из описанных рисков формируется стратегия контрмер.

Результатом шага будет один документ:«Стратегия контрмер».

Зонирование сети

Одной из успешных практик, которая позволяет успешно анализировать и уменьшать риски является зонирование сети. ИТ инфраструктура логически делится на зоны с различными компонентами и требованиями к защите – частная зона содержит активы, полностью контролируемые корпорацией; публичная зона, содержит активы с которой взаимодействуют внешние к корпорации клиенты.

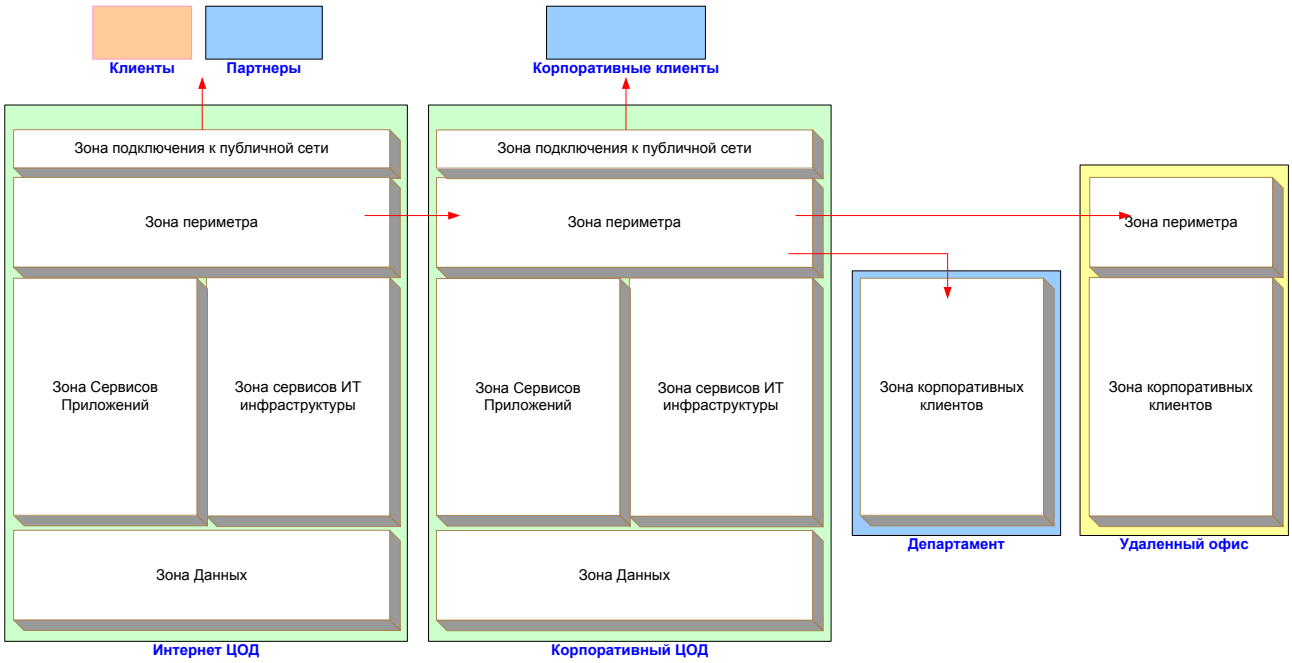

Рис. 2. Зонирование сети корпорации

Архитектура безопасности предполагает использовать 6 зон безопасности (табл. 1).

Таблица 1

Зоны безопасности корпорации

Название зоны	Описание
Зона подключения к публичной сети	Содержит системы подключения к публичной сети, системы защиты и инспекции сетевого потока.
Зона периметра	Содержит системы для удаленного подключения, кэширования содержания, сервера приложений презентационного уровня.
Зона приложений	Содержит сервера приложений и сервера управления базами данных.
Зона сервисов ИТ инфраструктуры	Содержит системы управления защитой, сетью, пользователями и ИТ инфраструктурой.
Зона данных	Содержит системы хранения данных, резервного копирования и восстановления.
Зона корпоративных клиентов	Содержит рабочие станции и устройства сотрудников компании.

Между зонами определены и реализованы ограничения, указанные в таблице 2.

Таблица 2

Ограничения между зонами безопасности корпорации

Зона источник	Зона назначения	Ограничения
Public	Private	Устройство для анализа сетевых пакетов расположено между зонами.
Public	Private	Только сетевой трафик портов 80 и 443 разрешен для прохождения между зонами.
Public	N/A	Если пользователи аутентифицируют себя любому уровню этой зоны, уровень должен обеспечить шифрованный канал для обмена информацией.

Другая практика уменьшения рисков – эшелонная защита – предполагает, что контрмеры создаются на пяти уровнях ИТ инфраструктуры:

1. Уровень физического доступа.
2. Уровень сети.
3. Уровень узла.
4. Уровень прикладных программ.
5. Уровень данных.

Рис. 3 Уровни эшелонной защиты в корпорации

Поскольку в большинстве случаев для осуществления атаки агенту необходимо использовать или обойти несколько уровней, размещение контрмер на всех уровнях позволяет значительно уменьшить риск. Как пример, ИТ инфраструктура Корпорации должна оставаться защищенной при отключении систем сетевой защиты (firewall).

Технологии защиты

Каждый компонент ИТ инфраструктуры включает в себя механизмы защиты. Список всех механизмов можно отобразить в виде таблицы 3.

Таблица 3

Механизмы защиты

Механизмы защиты	**Типы рисков**
Уровень приложений	
HTML content filters	Идентифицирует и реагирует на неавторизованные URL строки.
Уровень данных	
Авторизация (NTFS ACL)	Запрещает доступ к данным для неавторизованных клиентов.
Шифрование (IPSec, EFS, SSL)	Уменьшает риск прослушивания информации в сети и чтения данных с носителей в обход механизмов авторизации.
Уровень узла	
Internet Information Services (IIS) 6.0 Hardening	Обеспечивает дополнительный уровень защиты для сервера приложенийIIS 6.0, помогает избежать ошибок при конфигурации.
Windows Server 2003 шаблоны безопасности	Приводит систему к базовому уровню защищенности, путем настройки более чем 1200 параметров.
Уровень сети	
Firewalls	Сетевые экраны обеспечивают инспекцию сетевого трафика и располагаются между сетевыми зонами.
Internet Protocol Security (IPSec)	Защищает целостности и конфиденциальность сетевого трафика.
Уровень физического доступа	
Контроль физического доступа	Контролируемый доступ в помещения и этажи Корпорации.
Турникет	Контроль доступа на территорию Корпорации.

Управление

Архитектура безопасности должна быть управляемой и включать в себя соответствующий персонал, процессы и технологии. Управление безопасностью описано в методологии MOF (табл. 4).

Таблица 4

Роли в архитектуре безопасности

MOF ролевой кластер	**Наименование роли**
Operations, Release, Infrastructure, Support, Security	Менеджер безопасности Менеджер безопасности по работе с персоналом Инженер безопасности операционных систем Инженер безопасности аппаратного обеспечения Инженер безопасности сети Инженер безопасности физического доступа Менеджер по работе с внешними подрядчиками Аудитор безопасности

Выводы

При разработке архитектуры безопасности ИТ инфраструктуры можно выделить следующие критерии для оценки качества системы:

1. Управляемость

Управляемость, пожалуй, является определяющим свойством системы безопасности. Неуправляемую систему безопасности очень трудно защитить без использования механизмов мониторинга - потенциальные нарушения защиты могут остаться незамеченными. Без диагностирования труднее решать вопросы безопасности .

Подход с применением зон, принятый для системы безопасности, также может использоваться для ее управления. Каждую зону безопасности можно рассматривать как область управления, а задачу по управлению безопасностью можно поручить в случае необходимости локальным администраторам. На сегодняшний день для большинства устройств защиты существует возможность удаленного управления, поскольку они могут связываться с консолью централизованного управления, с помощью которой выполняется мониторинг их работы и налаживание конфигураций.

2. Использование административных ролей

Модель команд MOF (Microsoft Operations Framework) предлагает рекомендации для управления ИТ - службами, созданные на основе опыта успешных организаций различного масштаба, которые применяют ИТ - технологии в своей деятельности от крупных корпоративных ИТ - отделовдо небольших дата- центров электронной коммерции и поставщиков служб приложений .

В MOF определены кластеры ролей, каждый из которых связан с определенным аспектом ИТ -операций. Роли кластера Безопасность (Security role cluster) призваны обеспечивать конфиденциальность, целостность и доступность данных предприятия. Специалисты по безопасности, которые выполняют эти роли, уделяют внимание не только техническим проблемам, связанным с защитой корпоративной сети, но и политике и практике бизнеса. Речь идет об электронной почте организации, применения удаленного доступа, предоставления разрешений на использование важной корпоративной финансовой информации и личных данных работников, а также о таких специфических вопросах, как обеспечение конфиденциальности списка телефонов работников организации .

Особо отметим следующее.

Работники, которые выполняют роли по управлению и для которых предусмотрен высокий уровень доступа на предприятии, могут получить доступ к важнейшей информации. Таких работников следует тщательно подбирать, поскольку они сами могут представлять угрозу безопасности.

Роли в кластере безопасность выполняют следующие общие обязанности:

• помощь в мониторинге правильности работы ИТ-ресурсов;

• обнаружения вторжений и защита от вирусов;

• предоставление защиты путем отказа от обслуживания;

• определение политик скрытия и безопасной передачи данных;

• выполнение аудита и составления отчетов о его результатах;

• проектирование эффективной системы безопасности и системы управления для сетевых доменов;

• тестирование и внедрение стратегических технологий защиты;

• мониторинг и оценка уязвимостей сети;

• обеспечение быстрого реагирования на вторжение в реальном времени;

• управления инфраструктурой открытых ключей;

• управление требованиями IP- безопасности;

• управление требованиями проверки подлинности и доступа;

• управления применением и требованиями политик в отношении пользователей (например , политикой применения паролей);

• управление внешними и физическими требованиями к безопасности (например, доступом в компьютерные лаборатории);

• управления требованиями к безопасному обмена сообщениями;

• предоставление текущей технической поддержки и консультаций по соответствующим вопросам для различных инициатив по поддержанию безопасности в организации.

3. Системное администрирование

Централизованный подход к администрированию системы безопасности является достаточно простым для применения менеджером по безопасности , поскольку все задачи сосредоточены в одном месте. Однако архитектура системы безопасности может сделать удаленное управление невозможным из-за определенных ограничений безопасности.

Для удаленного адмистрирования применяют средства трех типов:

• консольММС (Microsoft Management Console);

• веб - инструменты;

• средства сторонних производителей.

Обычно большая часть функций удаленного управления осуществляется с по-мощью консоли ММС и средств сторонних производителей. Веб - инструменты постоянно совершенствуются.

Безопасность также в определенной степени зависит от распространения удаленного программного обеспечения, в частности от того , насколько оперативно происходит обновление программного обеспечения клиентов виртуальных частных сетей и антивирусных программ. Системное администрирование средств, которые используются для реализации безопасности и защиты ярусов , может оказаться сложным заданием. Когда в организации принята стратегия глубокоешелованной защиты , это приводит к росту сложности управления средой в зависимости от значимости компонентов. При условии, что много разных администраторов управлют различными технологиями, применяемыми в среде, внесение изменений может привести к многочисленным случаям неправильного настройки конфигураций. Для уменьшения такого риска в среде должны быть введены надежные процессы обмена данными и управления изменениями. На рынке появляются инструментальные средства для управления политиками безопасности для различных технологий, но пока они несовершенны.

4. Производительность

Производительность системы безопасности в первую очередь зависит от того, какие технологии и ограничения реализованы в среде.

• **Фильтрация пакетов на сетевом уровне.** Почти во всех ситуациях фильтрация пакетов увеличивает время их передачи из исходного места к месту назначения. Задержка зависит от способа проверки пакетов. Например , частые проверки с помощью механизма прокси на уровне прикладных программ занимают больше времени, чем простая фильтрация портов, поскольку такой процесс требует более глубокого исследования пакетов.

• **Шифрование**. Шифрование данных всегда приводит к передаче большего количества данных, а также создает дополнительную нагрузку на процессоры устройств, выполняющих шифрование и дешифрование. Такие нагрузки могут быть переведены на специальные средства аппаратного обеспечения.

5. Консолидация

Какой будет система безопасности - разрозненной или консолидированной, определяется архитектурами сетей и программного обеспечения, которые она поддерживает. Облегчения управления системой безопасности является определяющим фактором консолидации серверных и сетевых устройств. Но консолидация должна выполняться с учетом требований к безопасности данных и структуры зон, разработанной для поддержки безопасности.

Консолидируя службы на меньшем количестве серверов, необходимо принять во внимание следующее:

• Обеспечивает ли консолидация по-режнему, автономное администрирование служб на совместно используемом сервере, если до этого администрирование этими службами выполняли разные лица?

• Какие дополнительные риски (для сервера , на котором уже выполняются эти службы , или для приложений, для которых, существуют свои риски) создает эта новая служба или приложение? Или организация готова согласится с таким дополнительными рисками ?

• Не выдвигают ли различные требования к паролям и / или шифрованию приложения или службы? Если да, то они не совсем пригодны для консолидации.

• Не используют ли приложения или службы разные учетные записи служб или повышенные привилегии, которые могут предоставить нападающему, который получит несанкционированный доступ к одной службе, доступ к информации, выполняемой в других процессах на том же сервере?

6. Стандарты и инструкции

Стандарт ISO 17799 - это принятый на международном уровне ряд регуляторных норм, которые объединяют лучшие практики в сфере безопасности информации. Это стандарт создан на основе английского стандарта BS 7799, который он постепенно вытеснил.

ЛИТЕРАТУРА

1. Информационные технологии – практические правила управления информационной безопасностью //ISO/IEC 17799 МЕЖДУНАРОДНЫЙ СТАНДАРТ - Первое издание 2000-12-01-87 с.

2. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.

3. Засади регіональної інформатизації/ Довгий С.О., Копійка О.В., Черепін Ю.Т.- К.:ВПЦ «ТИРАЖ», 2004. –304 с.

4. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития/ С.А.Довгий, О.В.Копейка, С.П.Поленок. – К.:Укртелеком, 2001. – 281 с.

5. O.Kopeika, I.Tarasenko, A.Kisselevskiy, A.Karichenskiy, T.Valiulin Softline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom// TM Forum Case Study Handbook, Volume 3, May 2007 – P. 27

6. [Електронний ресурс]. - Режим доступу: http://www.tiaonline.org/standards/

7. Jew, Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010- page 28.

8. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric – page 4.

9. Telecommunications Infrastructure Standard for Data Centers//TIA STANDARD TIA-942. TELECOMMUNICATIONS INDUSTRY ASSOCIATION - April 2005. - P. 135

10. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices// Committee Approval - January 2011 First Published: March 2011 - P. 367

Надійшла: 25.02.2014 р. Рецензент: д.т.н., проф. Розорінов Г.М.