

А.А.СКОПА, докт.техн.наук, доц., зав.каф. ОНЭУ, Одесса

Н.Ф.КАЗАКОВА, канд.техн.наук, доц., ОНЭУ, Одесса

С.Т.СОРОКА, зам.нач. Центра обработки данных, Одесский филиал ОАО «Укртелеком»

ПОЛИТИКА ПРЕДУПРЕЖДЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ОДЕССКОГО ФИЛИАЛА ОАО «УКРТЕЛЕКОМ»

Викладаються основні відомості про політику попередження загроз інформаційній безпеці (інциденти) в практичній діяльності Одеської філії ВАТ «Укртелеком».

Ключові слова: інцидент, безпека, укртелеком, моніторинг, it-ресурс, інфраструктура

Излагаются основные сведения о политике предупреждения угроз информационной безопасности (инцидентов) в практической деятельности Одесского филиала ОАО «Укртелеком».

Ключевые слова: инцидент, безопасность, укртелеком, мониторинг, it-ресурс, инфраструктура

Basic information is expounded about the policy of warning of incidents in practical activity in Odessa branch joint stock company «Ukrtelecom».

Keywords: incident, security, ukrtelecom, monitoring, it-resources, infrastructure

Введением, постановкой проблемы в общем виде и ее связь с важными научными и практическими заданиями является задача освещения практической деятельности Центра обработки данных Одесского филиала ОАО «Укртелеком» по внедрению политики предупреждения инцидентов, связанных с посторонним вмешательством в деятельность автоматизированных, компьютеризованных и автоматических служб. Исходя из этого, **целью статьи** является изложение основных сведений о политике предупреждения угроз информационной безопасности (инцидентов) в практической деятельности Одесского филиала ОАО «Укртелеком».

В 2007 году ОАО «Укртелеком» создало территориально-разделенный Центр обработки данных (ЦОД). Внедрение проекта осуществляли компании S&T «Софт-Троник» и «Майкрософт Украина». Главный ЦОД находится в Киеве. Также имеются ЦОД в Днепропетровске, Львове, Харькове, Одессе, Донецке и Харькове. На сегодняшний день введены в действие практически все службы ЦОД. Сотрудники ОАО «Укртелеком» получили доступ к таким сервисам как сетевые сервисы, служба активного каталога, электронная почта, хранение файлов. Во время реализации были использованы системы хранения данных EMC, сервисные решения Hewlett-Packard, сетевое оборудование Cisco, программные продукты Microsoft. Оценка Генерального директора компании «Майкрософт-Украина» Валерия Лановенко – аналогичных проектов в мире еще нет.

ЦОД позволяет ОАО «Укртелеком» вводить новые бизнес- и корпоративные сервисы с возможностью их автоматизации в рамках компании. Один из наиболее

важных результатов проекта – создание корпоративного портала на базе продуктов Microsoft. Сегодня каждый сотрудник ОАО «Укртелеком» (в том числе Одесского филиала ОАО «Укртелеком») получил возможность доступа ко всем необходимым ему сервисам (в том числе к автоматизированным системам) непосредственно со своего рабочего места.

Анализ исследований и публикаций

Международные стандарты, взятые за основу проектных решений для ЦОД Одесского филиала ОАО «Укртелеком», следует рассматривать как сбалансированный ряд организационных, организационно-технических, а также значительный набор технических мер, основанных на реальной мировой практике [2].

В настоящее время не существует единого стандарта, где были бы определены требования к ЦОД. В Украине и России действующих ЦОД еще слишком мало, чтобы делать обобщения, поэтому приходится использовать зарубежные опыт и модели расчетов.

Стандартизация рассматривается как один из принципов системного подхода к построению инфраструктуры, обеспечивающий масштабируемость решений и сокращение капитальных расходов. Она помогает унифицировать реализацию взаимосвязанных инфраструктурных систем ЦОД. Сейчас проектирование и планирование ЦОД регламентируется американским стандартом ANSI TIA/EIA-942, утвержденным в апреле 2005 г. Это единственный комплексный стандарт, где освещается широкий круг вопросов, связанных с организацией ЦОД. Он предлагает последовательный подход к решению задач по созданию ЦОД [3].

Комплексных европейских и международных аналогов не существует, однако, как предполагается, ISO возьмет его за основу при разработке соответствующего международного стандарта. Стандарт обобщает многолетний опыт создания ЦОД. Следование его рекомендациям позволяет максимально приблизиться к уровню надежности с заветными пятью девятками – 99,999% [4]. Ряд требований в ЦОД Одесского филиала ОАО «Укртелеком» (как и во всем ОАО «Укртелеком») принято в качестве постулата.

Изложение основного материала

В процессе практического создания этой мощной информационной структуры в ЦОД Одесского филиала ОАО «Укртелеком» возникли ряд проблем и вопросов, что является нормальным явлением так называемой «привязки» теоретических разработок и объективной реальности.

Система эксплуатации ЦОД предназначена для организации эффективного управления IT-ресурсами и компонентами инфраструктуры ЦОД. Основными задачами системы эксплуатации являются повышение надежности, обеспечение заданной производительности и необходимых технико-эксплуатационных параметров инфраструктуры ЦОД. В таблице отражена тенденция роста случаев нарушения безопасности, происходящих каждый год по данным, поступающим в координационный центр CERT® (экспертный центр по Интернет-безопасности).

Таблица . Тенденция роста случаев нарушения безопасности

Год	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Число замеченных происшествий	2340	2412	2573	2134	3734	9853	21756	55108	82004	113204*	143618*	171412*	162239*	163775*	177307*	190012*

Примечание: Сведения о нарушениях безопасности после 2003 года координационным центром CERT® не публиковались и в таблице приведены данные, полученные авторами из открытых источников в сети Интернет

Информационная безопасность включает в себя шесть основных элементов ее детализации: задачи безопасности по конфиденциальности, целостность и доступность информации «системы», цели безопасности, спецификация функций безопасности и описание механизмов безопасности.

Основа информационной безопасности ЦОД Одесского филиала ОАО «Укртелеком» – процессный подход к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СИБ (система информационной безопасности) предприятия. Он заключается в создании и применении системы процессов управления, которые взаимосвязаны в непрерывный цикл планирования, внедрения, проверки и улучшения СИБ (рис.1 [1]).

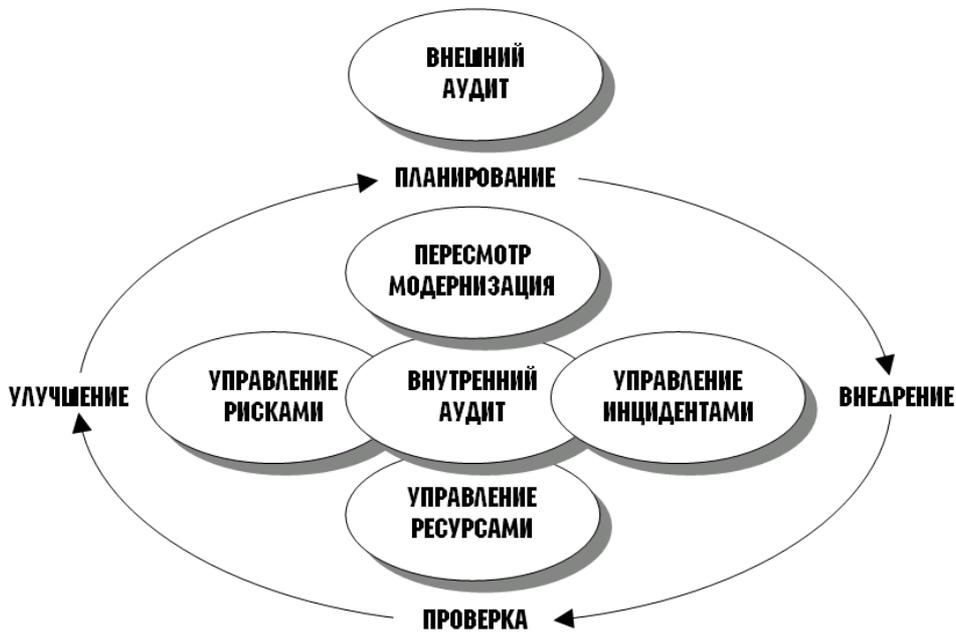


Рис. 1. Процессный подход в рамках СИБ

Основным движущим механизмом СИБ является периодический анализ рисков информационной безопасности. Высшее руководство организации также вовлекается в процесс управления СИБ посредством принятия решений на основе результатов анализа рисков, результатов внутренних аудитов и других механизмов СИБ.

Политика информационной безопасности ЦОД Одесского филиала ОАО «Укртелеком» – это не только частичное ограничение доступа: не менее важным аспектом является эффективное распространение информации об инцидентах среди сотрудников предприятия. И здесь на первый план выходит требование по обеспечению того, чтобы в нужный момент нужная информация была доступна для анализа.

СИБ ЦОД Одесского филиала ОАО «Укртелеком» представляют собой решение, направленное на обеспечение защиты критичной информации организации от разглашения, утечки, несанкционированного доступа и объединяет в себе комплекс организационных и организационно-технических мероприятий.

В процессе отработки проектных решений возникла необходимость создания с учетом требований действующих законодательных, нормативных, нормативно-технических документов в Центре информационных технологий и технического обеспечения (ЦИТ ТО) Одесского филиала ОАО «Укртелеком» СИБ, утвержденной решением техсовета.

Система создана без дополнительных финансовых вложений, увеличения штатного состава и привлечения сторонних организаций, обеспечивая необходимый уровень информационной безопасности (ИБ), которая состоит из трёх основных компонентов: конфиденциальность, целостность, доступность.

Для формализации указанных проблем В ЦИТ ТО ведется разработка организационно-методических документов: «Обеспечение информационной безопасности в центре обработки данных» и «Политика предупреждения инцидентов в ИТ-инфраструктурах», в которых администраторы ИТ-инфраструктур найдут необходимые для использования в повседневной деятельности организационные и организационно-технические меры предупреждения инцидентов и реагирования на них.

Предпосылкой создания приведенных разработок послужило создание в ОАО «Укртелеком» развернутой комплексной сети Центров обработки данных (ЦОД).

Указанные разработки являются интеллектуальной собственностью авторов статьи и коллектива ЦОД ОАО «Укртелеком», которая защищена Законом Украины «Об авторском праве» (ст. 9 разд.2).

Международные стандарты, взятые за основу рекомендаций, следует рассматривать как сбалансированный ряд организационных, организационно-технических, а также значительный набор технических мер, основанных на реальной мировой практике. Использование рекомендаций стандартов исключает возможность повторения известных ошибок и, в известной степени, позволяет создавать, сопровождать и контролировать состояние различных ветвей ИТ-инфраструктур. Предупреждение инцидентов, реагирование на проблемы – составные части системы информационной безопасности. Усилия, затраченные на создание системы информационной безопасностью, позволят организации выйти на новый уровень отношений с клиентами и продемонстрировать надежность ОАО «Укртелеком».

Подробнее следует остановиться на основных положениях указанных документов.

Одной из наиболее ответственных и сложных задач, решаемых в процессе создания СИБ, следует назвать проведение анализа рисков информационной безопасности в отношении активов организации в выбранной области деятельности и принятие высшим руководством решения о выборе мер противодействия выявленным рискам.

Анализ рисков – это основной движущий процесс СИБ. Он выполняется не только при создании СИБ, но и периодически при изменении бизнес-процессов организации и требований по безопасности.

В процессе анализа рисков для каждого из активов или группы активов производится идентификация возможных угроз и уязвимостей, оценивается вероятность реализации каждой из угроз и, с учетом величины возможного ущерба для актива, определяется величина риска, отражающая критичность той или иной угрозы.

Поскольку архитектура инфраструктуры поддерживают сетевые устройства, так и устройства пользователей, в силу самого этого факта, если нарушается их безопасность, то потенциально может выйти из строя вся сеть и ее ресурсы.

СИБ ЦОДа выполняет общие требования к поддержанию защищенности информационной системы (ИС):

- обеспечение конфиденциальности финансовой информации, почтовой переписки, информации о проектах и/или заказчиках;
- обеспечение непрерывности ведения технологического процесса;
- выполнения обязательств перед пользователями.

Алгоритм деятельности ЦОД ОАО «Укртелеком» в упрощенном варианте приведен на рис. 2.

Некоторые технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер. Другие могут быть встроены в программы. Некоторые же выполняются людьми и являются реализацией указаний руководства, содержащихся в соответствующих руководящих документах.

Принятие решения о выборе уровня сложности технологий для защиты системы требует установления критичности информации и последующего определения адекватного уровня безопасности.



Рис. 2. Алгоритм деятельности ЦОД

Основной причиной наличия потерь, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие обширных знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого. Осведомленность конечного пользователя о мерах безопасности обеспечивает четыре уровня защиты компьютерных и информационных ресурсов:

Предотвращение – только авторизованный персонал имеет доступ к информации и технологии.

Обнаружение – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

Ограничение – уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению.

Восстановление – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Для защиты сетей и ИТ-инфраструктуры в ОАО «Укртелеком» используется комплексный подход, контроль всех уязвимых мест, а также соответствующих необходимых мер защиты.

Вместе с тем, как любая другая информационная система, информационно-телекоммуникационная инфраструктура подвержена влиянию нештатных ситуаций и угроз.

Предупреждение инцидентов, реагирование на проблемы – составные части системы информационной безопасности. Усилия, затраченные на создание системы информационной безопасностью, позволят ИТ-организации выйти на новый уровень отношений с клиентами.

Выводы

Приведенный материал дает возможность системного понимания рекомендаций международных стандартов для реализации политики предупреждения инцидентов.

Использование передового опыта, реальных мер по предупреждению инцидентов в ИТ-инфраструктурах, основанных на мировой практике, международных стандартов, безусловно, необходимо так же, как использование новых компьютерных технологий, аппаратного и программного обеспечения.

Список литературы: 1. *Носаков В.* Создание комплексной системы управления информационной безопасностью // [Электронный ресурс]: http://www.jetinfo.ru/jetinfo_arhiv/?pid=17a12802a5b1a432d8036cef1f75dc15&nid=9127a7829a18346ad045a73263b3_8ab4#PIC1-1. 2. *Скопа О.О., Казакова Н.Ф.* Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем // Системи обробки інформації. – Випуск №7(79): Безпека та захист інформації в інформаційних системах. – Харків: Харківський ун-т Повітряних Сил ім.І.Кожедуба. – 2009. – С.48-54. 3. *Казакова Н.Ф., Тимофеев Б.В.* Аналіз захищеності інформаційних мереж // Комп'ютерні технології, інформаційна безпека та дизайн: Матеріали IV наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного ун-ту (секції 7...13), 22 травня 2009 р. – Одеса: МГУ, 2009. – С.71-73. 4. *Скопа О.О., Казакова Н.Ф.* Глобальні властивості нейронних мереж / Наукові записки УНДІЗ. – №3(5). – К.: УНДІЗ, 2008. – С.13-19.

Поступила в редколлегию 21.03.2012