СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ - СВИЩОВ
КАТЕДРА „СЧЕТОВОДНА ОТЧЕТНОСТ“

МЕЖДУНАРОДНА НАУЧНО-ПРАКТИЧЕСКА КОНФЕРЕНЦИЯ

СЧЕТОВОДСТВОТО И ОДИТА В УСЛОВИЯТА НА ИНФОРМАЦИОННАТА ГЛОБАЛИЗАЦИЯ

СБОРНИК НАУЧНИ СТАТИИ

4-5 ноември 2009 г.
Свищов

УЧЕТ ЗАТРАТ НА УСТРАНЕНИЕ ИНФОРМАЦИОННЫХ ИНЦИДЕНТОВ

Д.э.н., профессор, Татьяна Мишова,
Д.э.н., профессор, Сергей Охрименко,
MCP, Константин Склифос,
магистр, Виталий Спынаки,
Лаборатория информационной безопасности
Молдавская Экономическая Академия
www.security.ase.md

Введение

В настоящее время большинство работ, связанных с исследованиями в области проблем информационной безопасности носит сугубо технический характер и ориентировано, главным образом, на решение задач защиты информационных ресурсов от несанкционированного доступа и противодействия атакам на информационные системы. Данные исследования связаны, в основном, с анализом влияния таких факторов, как правовые, организационные, технологические, технические. В то же время, недостаточно внимания уделяется анализу влияния экономических факторов, значение которых в настоящее время многократно возрастает.

Ключевыми вопросами информационной безопасности являются:

- что защищать?
- от чего (кого) защищать?
- как защищать?

Поиск ответов на приведенные вопросы связан с существенными затратами, которые несет владелец информационной системы и информационных ресурсов.

Практика функционирования систем информационной безопасности свидетельствует, что возникают определенные сложности прикладного характера в определении использования средств покрытия существующих рисков с точки зрения экономического обоснования (достаточности и эффективности).

Стоимостные аспекты деятельности информационных систем в части предоставления работ (услуг) определяют необходимость управления затратами. Данное условие действует также применительно к сфере устранения информационных инцидентов, поскольку управление

затратами напрямую участвует в формировании прибыли, как в краткосрочном, так и долгосрочном периоде.

При управлении затратами необходимо учитывать технологические и экономические особенности. Существующие методы управления затратами не в полной мере позволяют учитывать данные особенности [7]. Возникает необходимость в разработке методов управления затратами на устранение инцидентов, учитывающих технологические и экономические особенности.

Проблема управления затратами в информационных системах является относительно новой и требует обоснования необходимости разработки организации учета, методов калькулирования себестоимости отдельных комплексов работ и услуг. До настоящего времени недостаточно разработаны вопросы экономической сущности, структуры и классификации затрат, порядка их отражения, распределения косвенных затрат, анализа и планирования расходов.

Указанная проблема управления затратами связана, с одной стороны, с необходимостью снижения затрат и себестоимости, с другой – существованием группы затрат, в первую очередь, затрат на обеспечение информационной безопасности, снижение которой недопустимо.

Главенствующую роль в методологии стоимостного подхода играет оценка стоимости бизнеса. Теория и практика деятельности информационных систем использует следующие основные подходы:

- доходный подход (Income Approach);
- сравнительный подход (Market Approach);
- затратный подход (Asset Based Approach);
- оценка имущественных опционов.

Управление расходами может базироваться на двух стратегиях. Первая, получившая название «стратегии экономичности», основывается на минимизации затрат и включает следующие положения: все затраты и отдача представляются в денежной форме; принимаемые решения основываются на расчете денежных потоков; используемые активы следует разделять на две группы – активы, относящиеся к основному бизнесу, а также непрофильные активы. Первые следует развивать в соответствие с главной целью бизнеса, вторые сводить к минимуму.

Вторая стратегия, именуемая «стратегией результативности», предусматривает максимизацию отдачи затрат. Основами данной стратегии являются следующие положения:

- отдача не всегда может быть представлена в денежной форме;
- решения должны приниматься на основании комплекса критериев, характеризующих общую стратегию развития информационной системы;

- проводимая граница между активами (профильными и непрофильными) является условной;

- и, самое главное, принимаемые решения по минимизации затрат, соответственно и инвестиций, могут привести к существенным потерям в настоящее время и в будущем.

Главной целью настоящей работы является разработка методических основ учета затрат на устранение информационных инцидентов, которые должны включать рассмотрение следующих вопросов: определение информационного инцидента, этапов жизненного цикла инцидента, классификация и характеристика затрат и др. Разработка методических основ призвана обеспечить оценку:

- затратной части мероприятий по обеспечению информационной безопасности;

- эффективности функционирования системы информационной безопасности;

- инвестиционной привлекательности системы информационной безопасности [6].

Определение информационного инцидента (ИИ) и этапы жизненного цикла инцидента

Предпримем попытку дать определение информационного инцидента. Для этой цели используем разнообразные литературные источники [1-5, 9-13]. В соответствии с [3, с.251-252], совокупность действий, в результате которых произошло изменение информационного поля субъекта, определяется как информационная акция (ИА). Следует отметить, что цели проведения ИА могут быть самыми различными и зависеть от множества факторов, в числе которых можно выделить такие, как общее состояние информационного поля, состояние всех сторон, действующих в ИА (субъектов) и многие др.

Выделяется три основных типа ИА:

- ИА, предпринятая на своем информационном поле в целях обеспечения эффективной информационной поддержки целевому режиму функционирования системы, определяется как внутренняя ИА и является прямым информационным управлением;

- ИА, реализуемая на общем информационном поле в целях воздействия на выбранный элемент, является информационной атакой;

- ИА, предпринятая на общем информационном поле с целью обеспечения эффективной информационной поддержки целевому режиму функционирования системы, определяется как информационная защита.

Примерами ИА могут выступать:

- информирование – передача части информационной совокупности в пользование другой стороны;
- информационное давление – проведение информационных акций без санкций объекта воздействия;
- тиражирование информации – процесс распространения информационной совокупности;
- информационное нападение – информационная акция, предпринятая в общем информационном поле с целью противодействия;
- информационное обслуживание – проведение информационной акции с целью изменения информационной совокупности другой стороны;
- информационный прессинг – резкое увеличение интенсивности применения информационного воздействия;
- информационная агрессия – не объявленная информационная акция.

Считаем необходимым отметить, что приведенные определения требуют разработки соответствующей методики расчета затрат на устранение последствий информационного воздействия.

Другими словами, определены три типа акций – внутренняя, атака и защита. С точки зрения учета затрат нас будет интересовать два последних типа акций – атака и защита. В свою очередь, под атакой следует понимать несанкционированное воздействие на информационную систему и ее компоненты, программно осуществляемое по каналам связи. Выделяется два подтипа атак: первый направлен на инфраструктуру и протоколы сети, второй – на телекоммуникационные службы с использованием уязвимостей.

Класс атаки может быть представлен и описан следующими составляющими:

- характеристика атакующего объекта: расположение атакующего объекта (внутренний или внешний);
- атакуемый ресурс (по расположению – узловой, сетевой; по типу – пользовательские ресурсы, системные ресурсы, ресурсы СУБД, вычислительные ресурсы, ресурсы системы информационной безопасности);
- целевое воздействие на ресурс: сбор информации, получение прав пользователя ресурса, получение прав администратора ресурса, нарушение целостности ресурса, нарушение работоспособности ресурса и др.;
- признак характера атаки – распределенные, нераспределенные.

В соответствие с [5], основными этапами жизненного цикла ин-

цидента являются следующие:

- возникновение инцидента, т.е. время, когда сбой был автоматически или вручную обнаружен и поступила соответствующая информация;

- обнаружение, когда поставщик соответствующего сервиса проинформирован о сбое и затраченное на это время определяется как обнаружение;

- реагирование, период времени, необходимый для адекватного реагирования на инцидент, в рамках которого осуществляется диагностика, за которой следует выполнение «ремонтных» работ (прием информации, регистрация инцидента, классификация, составление, анализ и диагностика);

- «ремонт», комплекс действий по восстановлению соответствующих компонент, которые вызвали сбой, приведший к инциденту;

- восстановление, с помощью реализации таких работ, как конфигурирование и инициализация производится восстановление сервиса.

Средства обеспечения информационной безопасности

В стандарте ISO 7498-2 [8], определены пять базовых услуг для обеспечения безопасности информационных систем и сетей: конфиденциальность (Confidentiality), аутентификация (Authentication), целостность (Integrity), контроль доступа (Access Control), причастность ("неотпирательство", Nonrepudiation).

Конфиденциальность определяется как "свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных (неуполномоченных) личностей, объектов или процессов".

Аутентификация определяет два типа услуг: достоверность происхождения (источника) данных и достоверность собственно источника соединения или объекта коммуникации (peer-entity). Достоверность источника данных предполагает подтверждение того, что "источник полученных данных именно тот, который указан или объявлен".

Целостность имеет две базовые реализации: для сетей с установлением связи и без установления связи, каждая из которых может применяться для избранных групп информационных полей. Обеспечение целостности данных в сетях с установлением связи предполагает обнаружение "любой модификации, включения, удаления, или повторной передачи данных в последовательности (пакетов)".

Контроль доступа определяется как предотвращение неавторизованного использования ресурсов недопустимым способом. Данная ус-

луга не только обеспечивает доступ только авторизованных пользователей (и процессов), но и гарантирует указанные права доступа для авторизованных пользователей. Таким образом, эта слуга предотвращает неавторизованный доступ как "внутренних", так и "внешних" пользователей.

Причастность ("неотпирательство"). В стандарте ISO 7498-2 причастность определяется, как предотвращение возможности отказа одним из реальных участников коммуникаций от факта его полного или частичного участия в передаче данных. Определены две формы: причастность к посылке сообщения и подтверждение (доказательство) получения сообщения. Первая форма данной услуги предоставляет получателю доказательства, что сообщение было послано источником, его целостность не нарушена, на случай отказа отправителя от этого факта. Вторая форма причастности предоставляет источнику доказательства того, что данные были получены получателем, в случае попыток последнего отказаться от этого факта.

Доступность выступает в качестве основного сервиса безопасности. Она может быть предметом атаки злоумышленника с целью сделать ресурсы информационной системы недоступными или уровень их использования неудовлетворительными.

Для понимания того, как правильно управлять затратами в условиях устранения инцидентов, принципиальное значение имеет их обоснованная классификация в соответствии с требованиями управленческого учета. В соответствии с [7, с.25-29], выделяются затраты для принятия управленческих решений и для осуществления процесса контроля и регулирования.

Для формирования базового перечня затрат рассмотрим состав средств обеспечения информационной безопасности (рис.1). Данные средства могут быть разделены на две группы – встроенные и наложенные. Средства первой группы встраиваются в поставляемые системы, такие как операционные системы, системы управления базами данных, сетевые устройства, приложения и т.д.

Наложенные средства являются самостоятельными системами программной, аппаратной или смешанной реализации. Они приобретаются для создания комплексной системы обеспечения информационной безопасности и обладают достаточно большими функциональными возможностями.

Средства защиты информации от несанкционированного доступа классифицируются по четырем подсистемам [3, с.439-444]:

1. Подсистема управления доступом.

1.1. Средства идентификации, проверки подлинности и контроля

Рис.1. Состав средств защиты информации

доступа субъектов к ресурсам системы; к узлам сети, отдельным терминалам, внешним устройствам; программным ресурсам, каталогам, файлам и записям.1.2. Управление потоками информации.

2. Подсистема регистрации и учета.

2.1. Регистрация и учет: входа-выхода субъектов доступа; выдачи печатных выходных документов; запуска-завершения программ, заданий и задач; доступа к терминалам, узлам сети; каналам связи, внешним устройствам, программам, каталогам, файлам; изменения полномочий субъектов доступа; создаваемых защищаемых объектов доступа.

2.2. Учет носителей информации.

2.3. Обезличивание освобождаемых областей оперативной памяти и внешних накопителей.

2.4. Сообщения о попытках нарушения системы защиты.

3. Криптографическая подсистема.

3.1. Шифрование конфиденциальной информации.

3.2. Шифрование информации, принадлежащей различным субъектам доступа на различных ключах.

3.3. Использование сертифицированных криптографических средств.

4. Подсистема обеспечения целостности.

4.1. Обеспечение целостности программных средств и обрабатываемой информации.

4.2. Физический контроль и охрана средств вычислительной техники и носителей информации.

4.3. Служба администратора защиты информации в информационной системе.

4.4. Тестирование средств защиты информации.

4.5. Средства восстановления.

4.6. Сертифицированные средства защиты.

Наложенные средства обеспечения информационной безопасности объединяют средства управления доступом, средства фильтрации, средства защиты отдельных ресурсов, систему отражения вторжений и поиска уязвимостей, средства управления безопасностью сети.

К средствам управления доступом относят:

- аутентификацию (authentication) – использование входных паролей, специальные средства (токены), биометрические средства;
- авторизацию (authorization);
- управление идентификацией (identity management) – использование комплекса продуктов, предназначенных для унификации данных о пользователях, управления аутентификацией, авторизацией, профилями и правами пользователей, а также аудита доступа.

Средства фильтрации объединяют:

- межсетевые экраны (firewalls) – как система, реализующая политику контроля доступа;
- активный контекстный мониторинг/фильтрация (active content monitoring/filtering).

Данные средства исследуют всю информацию на возможность наличия разрушительных кодов или перекрестных ссылок. Примерами подобной деятельности являются:

- защита от распределенных атак типа «отказ в обслуживании» (antiDDoS tools) с помощью анализа аномалий, характерных для данного вида атак;
- защита от компьютерных червей (anti-worm solution), как набор средств для сдерживания инфицирования компьютеров;
- защита от спама (spam protection) , как набор программных средств для фильтрации входящей почты.

Средства защиты, использующие криптографические методы:

- удостоверяющий центр (certificate authority), как специализированная организация, выпускающая и управляющая сертификатами и открытыми ключами, которые используются для шифрования и дешифрования сообщений;
- шифрование файлов и сеансов связи (file and session encryption), как набор разнообразных алгоритмов для преобразования данных, не-

понятных неавторизованному пользователю;

- виртуальные частные сети и защищенные коммуникации (virtual private networks and cryptographic communications), как создание защищенных коммуникаций для мобильного взаимодействия;

- виртуальные частные сети на основе протокола SSL (SSL VPNs), с помощью которых обеспечивается защищенный удаленный доступ к корпоративным приложениям;

Средства защиты отдельных ресурсов интранет включают:

- защитные приложения (security appliances), как набор программного и аппаратного обеспечения;

- защищенные веб-серверы (secure Web servers), как набор средств защиты, обеспечивающих минимизацию лазеек для проникновения хакеров;

- защищенные веб-приложения (Web application security), как набор средств, защищающих от таких угроз, как фальсификация транзакций, подмена веб-страниц и др.

Системы отражения вторжений и поиска уязвимостей объединяют:

- системы предотвращения вторжений (intrusion prevention), как набор средств для автоматического блокирования действий злоумышленников и фиксации попыток осуществления атак;

-системное обнаружение вторжений (host-based intrusion detection), как комплекс программного обеспечения, основной целью которого является мониторинг информационной системы и приложений, выдача и реализация мер защиты;

- сетевое обнаружение вторжений (network-based intrusion detection), как набор средств сетевого обнаружения вторжений и выявление признаков, характерных для реализации попыток сканирования информационной системы, реализации атак типа «отказ в обслуживании» и т.д.;

- сетевые сканеры уязвимости (network-based vulnerability scanners), как набор специальных программ для моделирования поведения атакующей стороны и обнаружения уязвимостей;

- системные сканеры уязвимостей (host-based vulnerability scanners), программы проверки настройки информационных систем на соответствие принятой политике безопасности;

- сервисы безопасности: тесты на возможность проникновения (security services: penetration testing), набор средств для обнаружения слабых мест в системе информационной безопасности и выдачи рекомендаций по их устранению;

- уведомления о защите и реакции на инциденты в реальном времени (real-time security awareness/incident response), средства оценки эф-

фективности работы защитных механизмов в реальном времени.

Средства управления безопасностью сети включают:

- сервисы защиты: разработка политики безопасности (security services: policy development), как набор типовых примеров политик безопасности, который корректируется в зависимости от требований конкретной информационной системы;

- реализация политики безопасности организации (enterprise security policy implementation), как набор средств, позволяющих автоматизировать процесс управления политикой безопасности, включая создание, редактирование, усовершенствование, опубликование, доставку, обучение, аудит, отчетность и сопровождение;

- средства администрирования безопасности организации (enterprise security administration), как набор средств для организации условий выполнения прав и обязанностей персонала информационной системы;

- управляемые сервисы безопасности (managed security services), как набор средств для решения типовых задач администрирования вычислительной сети;

- автоматизированное управление защищенными обновлениями (path management systems), как комплекс средств управления установкой обновлений, с помощью которых устраняются обнаруженные в программном и аппаратном обеспечении уязвимости.

По нашему мнению, должны определяться также затраты на формирование ответной реакции на атаку, которые определяют наличие и использование встроенных механизмов ответной реакции – разрыв соединения с объектом, блокировка с помощью межсетевого экрана, отслеживание действий атакующего и др.

Представляется необходимым также моделирование и формирование затрат по линии «стоимости взлома» системы информационной безопасности [9,13]. Данный метод получил и другое название – анализ «стоимости болезни» (COI- Cost of Illness), используемый для учета и описания всех видов затрат по устранению последствий. Применительно к системе информационной безопасности «стоимость болезни» можно интерпретировать как «стоимость устранения инцидента». С помощью данного метода представляется возможным определение общих стоимостных границ комплекса мероприятий, выход за пределы которых свидетельствует о недостаточности проводимых мероприятий, либо их избыточности.

Суммарные затраты на создание и поддержку в работоспособном состоянии системы информационной безопасности складываются из затрат на создание самой системы и затрат на ликвидацию уязвимостей. Атака на информационную систему или успешный взлом, приводит к

потере работоспособности системы и информационных ресурсов (отказам), что в конечном итоге приводит к потере прибыли и требует значительных затрат по восстановлению. Достаточность и эффективность средств обеспечения безопасности определяется отношением затрат, понесенных по созданию системы и устранению уязвимостей к стоимости восстановления и потере прибыли.

Считаем возможным определить объем необходимых инвестиций в систему информационной безопасности для предотвращения атак, основываясь на [9-13].

Введем следующие переменные:

- угроза $T(t)$, характеризует количество атак в период t;

- уязвимость $V(t)$, характеризует вероятность совершения успешной атаки в периоде t;

- нарушение $\lambda(t)$- характеризует экономические потери после реализации атаки в период t;

- $T(t)\lambda(t)$ - потенциальные потери в единицу времени t в инвестиционный период $(t_j;t_{j+1})$, которые определяются следующим образом:

$$PL(t_j,t_{j+1}) = \int_{t_j}^{t_{j+1}} T(\tau)\lambda(\tau)d\tau; \qquad (1)$$

- риск безопасности в единицу времени $T(t)V(t)$;

Для инвестиционного периода (t_j,t_{j+1}) риск безопасности определяется как

$$SR(t_j,t_{j+1}) = \int_{t_j}^{t_{j+1}} V(z_j;\tau)T(\tau)d\tau, \qquad (2)$$

Где z_j- инвестиции в период $(t_j;t_{j+1})$. Полученная уязвимость $V(z_j;t)$ увеличивается во времени.

Введем следующие стохастические переменные:

A - количество атак в единицу времени периода t; Данная переменная является дискретным и целым числом, функция плотности распределения вероятности равна

$$P_A(n;t) = \Pr\{A = n;t\}, \qquad (3)$$

То есть вероятность того, что A равняется n в периоде t. Ожидаемая ценность A принимает значение $E\{A\} = T(t)$.

S -число успешных атак в единицу времени интервала t. Данная переменная является дискретной, функция распределения плотности вероятности $P_S(m;t) = \Pr\{S = m;t\}$, то есть вероятность того, что S

равняется m в интервале t. Ценность S определяется как $E\{S\}$ и уязвимость $V(t) = \frac{E\{S\}}{E\{A\}}$ и $E\{S\} = T(t)V(t)$, то есть риск безопасности в единицу времени интервала t.

L - экономические потери вследствие успешного нападения в интервале t, непрерывная функция плотности распределения вероятности L определяется как $f_L(l;t)$, то есть вероятность того, что L попадает в интервал $(l; l+dl)$ в период t, равна $f_L(l;t)dl$. Ценность L может быть представлена как $E\{L\} = \lambda(t)$ в единицу времени.

Используя стохастические значения S и L, можно определить индивидуальные потери $L_1, L_2, L_3, \ldots$ в единицу времени t. Общая сумма потерь в единицу времени составляет

$$L_m = \sum_{i=1}^{m} L_i . \qquad (4)$$

Данное обобщение необходимо увязать с временной зависимостью $\lambda(t)$ и $V(t)$, поскольку угрозы, уязвимости и потери изменяются во времени.

Заключение

Приведенный материал не исчерпывает всего многообразия вопросов и не позволяет дать ответы на них, поскольку данное направление исследований находится на стадии формирования целей и задач. Дальнейшие исследования должны быть связаны с развитием теоретических положений «самозащиты» и «самострахования», расширением соответствующего раздела политики безопасности по экономическому обоснованию и предсказуемости затрат на информационную безопасность, оптимизацией затрат при анализе информационных рисков и др.

Необходимо также формирование отдельного самостоятельного направления исследований по разработке адекватных экономико-математических моделей, описывающих взаимодействие компонент системы информационной безопасности информационной системы при реализации разнообразных инцидентов.

Литература

1. Девятин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. –М.: Радио и связь, 2006.

2. Джеймс Л. Фишинг. Техника компьютерных преступлений. - М: НТ Пресс, 2008.

3. Информационная безопасность открытых систем: В 2 т. Том 1 - Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2006.

4. Информационная безопасность систем организационного управления. Теоретические основы: В 2 т. – М.: Наука, 2006.

5. ИТ Сервис-менеджмент. Введение. 2002.

6. Охрименко С. Инвестиции в систему информационной безопасности. Management of Organizations – Finances, Production, Information/ Bielsko-Biala, 2009, p.274-281.

7. Управленческий учет: Учебно-практическое пособие.- Кишинэу; ACAP, 2000.

8. ISO 7498-2. Basic Reference Model - Part 2: Security Architecture. - February 1989.

9. N. Sklavos, P. Souras. Economic Model and Approaches in Information Security for Computer Networks. International Journal of Network Security, Vol.2, No 1, pp. 14-20, Jan.2006.

10. R. Hulthen. Communicating the Economic Value of Security Investments; Value of Security Risk.

8. L. A. Gordon, M. P. Loeb. The Economic of Information Security Investments. ACM Transaction on Information and System Security, 5, No 4, November 2002.

11. M. J. G van Eesten, J. M. Baurer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Working paper 2008/1.

12. Malicious Software (Malware): A Security Threat in the Internet Economy. Ministerial Background Report. DSTI/ICCP/REG (2007)5/Final.

13. P. Chen, G. Kataria, R. Krishnan. An Economic Analysis of the Strategic Interaction Among Computer Security Attackers.

ОРГАНИЗАЦИЯ УПРАВЛЕНЧЕСКОГО УЧЕТА
В УПРАВЛЕНИИ ЗАТРАТАМИ МАШИНОСТРОИТЕЛЬНОГО
ПРЕДПРИЯТИЯ
Лидия Костырко, д.э.н., профессор
Светлана Щеголькова, к.э.н., доцент 408

УПРАВЛЕНЧЕСКИЙ УЧЕТ РЕЗЕРВОВ ПРИБЫЛЬНОСТИ
ПРЕДПРИЯТИЯ
Руслан Костырко, кандидат экономических наук, доцент, ... 415

ФОРМЫ ОРГАНИЗАЦИИ БУХГАЛТЕРСКОГО УЧЕТА
В УСЛОВИЯХ ПРИМЕНЕНИЯ КОМПЬЮТЕРНЫХ
ТЕХНОЛОГИЙ
Наталья Костяник, Полтавский университет 424

ИССЛЕДОВАНИЕ ВЗАИМОСВЯЗИ КОНЦЕПТУАЛЬНЫХ
ПОДХОДОВ В УПРАВЛЕНИИ, УЧЕТЕ И АНАЛИЗЕ
Профессор, доктор экономических наук Инна Лазаришина 432

ПРОГНОСТИЧЕСКИЕ МЕТОДЫ ДИАГНОСТИКИ КРИЗИСНОЙ
СИТУАЦИИ И ОПРЕДЕЛЕНИЕ ПУТЕЙ ФИНАНСОВОЙ
СТАБИЛИЗАЦИИ ПРЕДПРИЯТИЙ
Владислав Левандовский 438

УЧЕТ ЗАТРАТ НА УСТРАНЕНИЕ ИНФОРМАЦИОННЫХ
ИНЦИДЕНТОВ
Д.э.н., профессор, Татьяна Мишова
Д.э.н., профессор, Сергей Охрименко
МСР, Константин Склифос
магистр, Виталий Спынаки 447

ФОРМИРОВАНИЕ ФИНАНСОВОГО РЕЗУЛЬТАТА
ПРЕДПРИЯТИЯ-БАНКРОТА
Новикова Наталья Евгеньевна 460

РАСХОДЫ И ЗАТРАТЫ КАК ОБЪЕКТЫ
БУХГАЛТЕРСКОГО УЧЕТА
Х. Ш. Нурмухамедова 464

АКАДЕМИЧНО ИЗДАТЕЛСТВО "ЦЕНОВ"

Управител: доц. д-р Богомил Трайков, тел. 0631/6 08 75
Зам. управител: Петър Папазов, тел. 0631/6 08 75
Дизайнер: Милена Александрова

СТОПАНСКА АКАДЕМИЯ "Д. А. ЦЕНОВ"
Свищов, ул. Ем. Чакъров, 2

АКАДЕМИЧНО ИЗДАТЕЛСТВО "ЦЕНОВ"
Свищов, ул. Градево, 24

МЕЖДУНАРОДНА НАУЧНО-ПРАКТИЧЕСКА КОНФЕРЕНЦИЯ

СЧЕТОВОДСТВОТО И ОДИТА В ИНФОРМАЦИОННАТА ГЛОБАЛИЗАЦИЯ

СБОРНИК НАУЧНИ СТАТИИ

Дадена за печат на 15.10.2009 г.
Печ. коли 40; формат 16/70/100; тираж 200 бр.

ISBN 978-954-23-0436-4

ПОЛИГРАФИЧЕСКА БАЗА
ПРИ АКАДЕМИЧНОТО ИЗДАТЕЛСТВО "ЦЕНОВ" – СВИЩОВ