ным, выполняются в первую очередь;
- сеть является «достаточно масштабной», чтобы заблокировать все узлы;
- одна распределенная сеть может предоставлять защиту множеству пользователей.

**4. Заключение**

Проблема DDoS-атак наиболее значимая в современном киберпространстве, поэтому различного уровня владельцы веб-ресурсов должны объединить свои усилия, чтобы найти максимально эффективное решение проблемы. Использование «Оверле́йной сети» является выгодным всем за счет ее независимого распределения от конкретного провайдера и невысокой цены для ее построения. Идея «Оверле́йной сети» может быть расширена путем использования в ее основе таких систем, как PlanetLab и GRID [2].

**Литература:**

1. Компьютерная документация от А до Я http://www.compdoc.ru/secur/xacer/what_is_ddos_attack/
2. Википедия – свободная энциклопедия http://wikipedia.org/
3. Internet – Technologies.RU http://www.internet-technologies.ru/articles/article_436.html
4. Angelos D. *Keromytis Network Security Lab Computer Science Department*, Columbia University «Denial of Service Attacks and Resilient Overlay Networks» http://www.nis-summer-school.eu/index.html
5. WebDocs.Ru документация от А до Я http://www.webdocs.ru/content-572.html

***Зинаида Гулка, Ольга Гешова,***
*Славянский университет Республики Молдова*

# ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

*Work deals with the actual scientific problems of information safety and protection of the information systems. Classification of the companies on a level of a maturity is given. In article are formulated requirements to information technologies under the control of internal threats with use of technique TCO (Total Cost Ownership)*

***Ключевые слова:*** *безопасность, мониторинг, информационная система*

Построение всеохватывающей системы информационной безопасности, минимизация рисков – процесс весьма сложный, длительный и дорогостоящий. В мире нет ни одной организации, которая внедрила бы

весь набор средств и реализовала все необходимые, описанные в стандартах, процессы. Выбор подходящих методов и степени защиты является субъективным процессом, лишь отчасти регламентируемым нормативными актами.

**Целью работы** является исследование особенностей формирования общей методологии безопасности IT- технологий, перспектив их международного развития.

**Предметом исследования** является изучение оценки эффективности инвестиций в системы информационной безопасности, производимых на основе методики TCO (Total Cost Ownership).

Приведём описание модели TCO для системы информационной безопасности (ИБ) Компании. Каждая модель TCO компании состоит из двух основных компонент: учетная карта предприятия и технический сценарий. Предложенная модель TCO для ИБ отличается от традиционной модели TCO тем, что в ней есть третий компонент – ***сценарий безопасности***.

**Учетная карта** TCO для ИБ предприятия состоит из пяти основных разделов: техническая часть, персонал, программное обеспечение, внешние службы, физическая безопасность. В свою очередь эти пять разделов подразделяются на следующие действия по безопасности: аутентификация, авторизация, защита кода и поддержка, реакция на Кибер-инциденты, мониторинг Контента, управление цифровыми правами, кодирование, брандмауэры, программа Информационной Безопасности, обнаружение Вторжения, соответствие Лицензии, регистрация, Сообщение и Аудит, управление Враждебным Программным Кодом, целостность Сообщения, управление секретностью, инфраструктура Открытых Ключей, сортировка Записей и Хранение, удаленный Доступ, оценка Рисков, управление Безопасностью, архитектура Безопасности, Сертификация Стандартов, управление Операционными Инцидентами Уязвимости, оценка и Управление.

**Вторая компонента TCO – технический сценарий** включает в себя: к**орпоративное резюме, IT профиль, сценарий безопасности**.

Для примера приведем данные из исследования, в которых показаны расходы типового финансово-кредитного органа на создание КРКИ на 5 лет:

***Таблица 2***

**Расходы на создание команды реагирования на Кибер-инциденты**

| ***Основные разделы*** | ***2004 г.*** | ***2005 г.*** | ***2006 г.*** | ***2007 г.*** | ***2008 г.*** | ***2009 (прогноз)*** |
|---|---|---|---|---|---|---|
| Технические средства | 30% | 37% | 35% | 33% | 31% | 29% |
| Персонал | 54% | 59% | 60% | 62% | 58% | 58% |
| Программное обеспечение | 14% | 3% | 4% | 3% | 10% | 12% |
| Внешние Услуги | 2% | 1% | 1% | 2% | 1% | 1% |
| **Итого:** | 100% | 100% | 100% | 100% | 100% | 100% |

Как видно из таблицы, наибольшие затраты связаны с персоналом.

На основе полученных результатов осуществляется подбор наиболее действенных способов и средств защиты. Выбор конкретного варианта защиты проводится с учетом критерия эффективность/стоимость. Проверка эффективности системы защиты должна носить периодический характер и включать оценку актуальности и полноты положений установленной политики безопасности.

Таким образом, рассмотренная методика (ТСО) может дополнительно включать и другие традиционные способы оценки эффективности, такие как скрытые и открытые проверки. Скрытыми проверками могут быть электронные письма с использованием методов социальной инженерии или мониторинг действий пользователей; открытыми – проведение тестирования, внешнего или внутреннего аудита. Однако, в целом, рассмотренная методика и её приложение на определение эффективности информационной защиты финансово-кредитного органа позволяет выявить наиболее приемлемый вариант использования собственных информационных ресурсов и обеспечения безопасной работы с коммерческой информацией.

**Литература:**

1. Киселев В.Д., Есиков О.В., Кислицын А.С. *Современные проблемы защиты в системах ее передачи и обработки* / Под ред. проф. Е.М. Сухарева. – М.: изд. «Солид», 2006. – С.200.
2. Середа С. *Программно-аппаратные системы защиты программного обеспечения*. – СПб.: Издательство BHV-Петербург, 2006. – 320 с.
3. http://www.it.ru – сайт компании АйТи.
4. http://bezpeka.com/ – оценка эффективности систем защиты информации.

***Денис Евтодиенко,***
*Министерство информационного развития*

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В связи со стремительным развитием информационных технологий в настоящее время защита персональных данных стала важным и актуальным вопросом для всех организаций. Персональные данные есть в отделе кадров, в бухгалтерии и даже в отделе продаж, что требует их защиты.

В связи с этим к персональным данным предъявляются основные требования информационной безопасности, такие как обеспечение целостности, доступности и конфиденциальности данных. Защита персональных данных должна достигаться путем исключения несанкциониро-