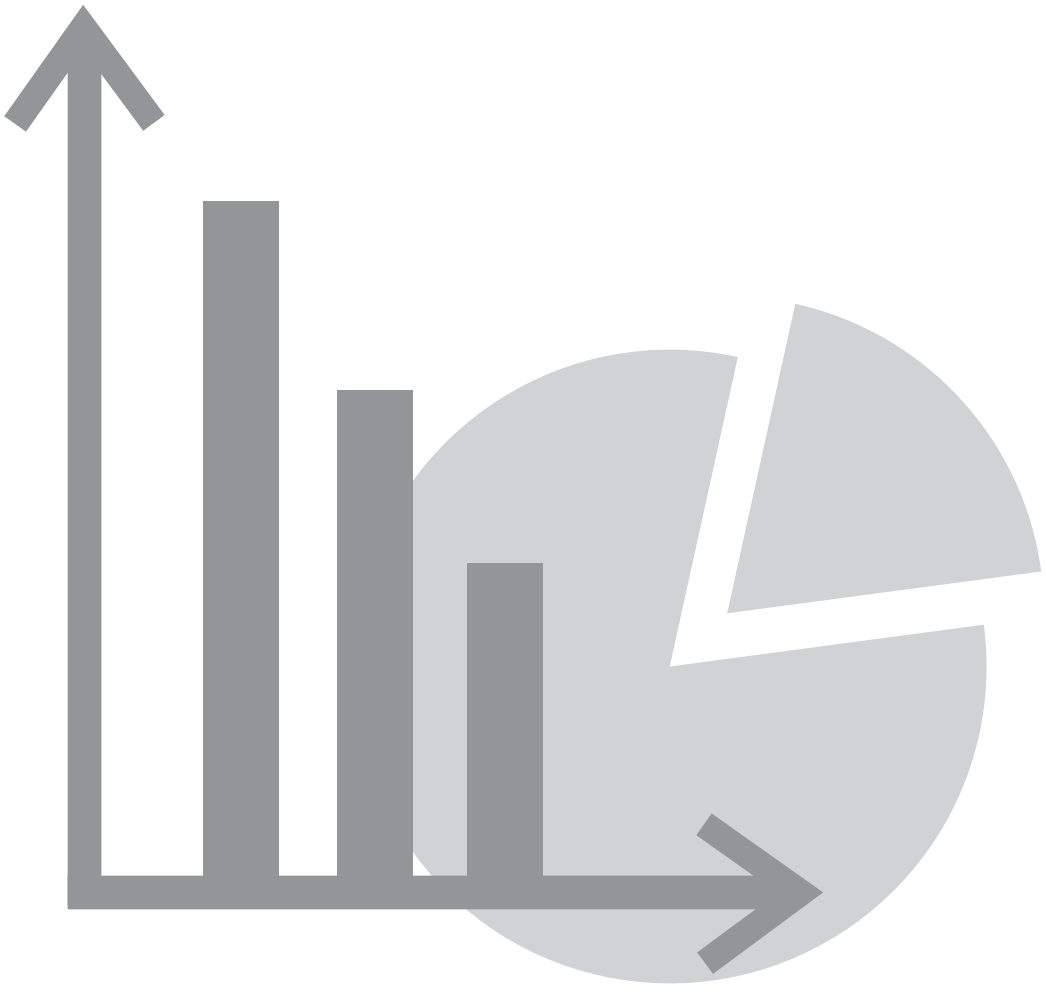
ISSP | Information Systems Security Partners

Аналитика

Анализ рентабельности инвестиций в автоматизированные комплексы веб-безопасности



Инвестиции в информационную безопасность

Инвестиции бизнеса сосредоточены в трех областях: технологии, люди, процессы. Относительные доли инвестиций в каждую из данных областей определяются природой бизнеса, рынком, экономикой, другими внешними и внутренними условиями.

Информационная безопасность (ИБ) сосредоточена сразу во всех областях, так как она является частью фундаментальной основы для роста активов, успешного протекания бизнес-процессов, управления человеческими ресурсами и становления компании на рынке.

Чем выше уровень угроз (нестабильная экономическая ситуация в стране, обостренная конкуренция, безработица и т.д.) – тем выше информационные риски, соответственно инвестиции в ИБ становятся более актуальными, более рентабельными, необходимыми.

Возврат (рентабельность) инвестиций рассматривается в двух категориях: в количественной и качественной (полезной).

Количественный возврат инвестиций

Определяет чистый денежный поток (cash Flow), со знаком «+», который мы получаем после внедрения технологии, а именно стоимость владения технологией, её окупаемость и получаемую прибыль от ее использования. Рассмотрим возврат инвестиций в течение 1го года.

Считается в несколько простых шагов: оценка рисков, оценка стоимости владения технологией, расчет дисконтированного денежного потока.

1. Нецелевое времяпровождение сотрудников в интернете.

Часто слышим: «зачем мне дома интернет, когда он у меня есть на работе…» это означает, что посещение сайтов развлечений, социальных сетей (одноклассники, вконтакте), видео-порталов, загрузка музыки, игр, фильмов, общение (ICQ, чаты) происходит в рабочее время.

По статистике в Украине, среднестатистический сотрудник тратит приблизительно два часа рабочего времени на поиск развлечений в интернете (четверть рабочего времени в день).
Предположим, зарплатный фонд в месяц составляет $ 300 000,00 в месяц с налогами и отчислениями. (500 сотрудников, средняя зарплата сотрудника $ 600).

Каждый месяц компания тратит $75 000 на то, чтобы сотрудники развлекались в интернете!

Динамическая база URL-категорий шлюзов веб-безопасности и политики доступа к ресурсам, обеспечивают эффективную фильтрацию посещаемых веб-сайтов и ограничение доступа к нецелевым (для бизнеса) категориям сайтов. Гибкие политики разграничения доступа (квоты по времени и трафику, ограничения скорости, предупреждения) позволят мягко и эффективно ограничить пользователей от нецелевого контента.

2. Угроза вирусного заражения.

По статистике, основная масса вирусов поступает именно через вредоносные сайты и объекты (документы, картинки), ссылки на которые содержатся на легитимных сайтах, в спам-рассылке и рекламных баннерах.

Наличие вируса, в корпоративной сети — ситуация форс-мажорная, и ущерб здесь очевиден — он равен убыткам от простоя сети на время проведения антивирусной зачистки плюс затраты на проведение этой зачистки. Например, суммарный ущерб только от одного вируса RedCode составил на сегодня $2,62 млрд., Love Bug $8,7 млрд. (KPMG, Computer Economics).
Комплексные и полиморфные черви и троянские программы используют уязвимости ПО и операционных систем пользовательских компьютеров. Поэтому, по статистике, организация в год испытывает несколько вирусных заражений, невзирая на установленные антивирусы на рабочих станциях

Итак, 2 заражения в год, предположим, по одной атаке в активное время: ноябрь и март. В организации из 500 пользователей, понадобится 250 человеко-часов администраторов на предотвращение последствий эпидемии.

*250 * $ 4 (стоимость часа специалиста) = $ 1000*

Время простоя = время пользователей + время простоя организации. Мы просчитаем лишь потерянное время пользователей. 50 человеко-часов на устранение проблемы при 2х специалистах (15 мин на каждый компьютер: диагностика+лечение). 1 час = 10 компьютеров.

$$\text{Время простоя (человеко} - \text{часы)} = \sum_{n=0}^{50} (500 - 10n)$$

Суммарное время простоя за 1 атаку будет 12 500 человека-часов. Что в денежном эквиваленте составляет $45000.

Итак, одна вирусная эпидемия в организации из 500 человек (рабочих станций), составляет $45000..

Автоматизированные комплексы веб-безопасности позволяют нивелировать риск попадания вирусов, червей и прочих угроз через веб-канал при помощи специализированных антивирусных движков, поведенческого анализа кода и превентивного блокирования доступа к зараженным сайтам.

3. Угроза информационных утечек и фишинг атак и мошенничества.

Мошенничество очень распространенное явление именно в веб. (Диаграмма 1) Чем более массовым становится веб-банкинг, тем больше будут происходить массовые рассылки, сайты-приманки и поддельные сайты.

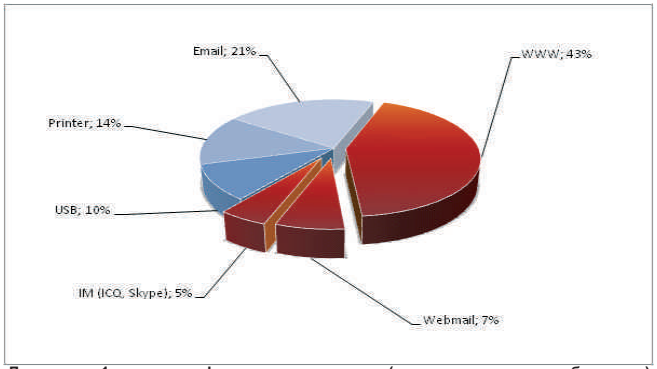


Диаграмма 1: каналы информационных утечек (красным отмечены веб-каналы)

Отправка номеров кредитных карт, передача электронных документов и другой чувствительной информации, больше чем в половине случаев, происходит по веб-каналам, с помощью мгновенных сообщений и личных почтовых ящиков в интернете.
Риск информационной утечки композитный и состоит из: стоимости реституции, юридических исков, затрат на восстановление репутации и отсроченный ущерб для бизнеса. Согласно исследованиям Forrester, составляющие прямых затрат на ликвидацию ущерба от утечки информации выглядят так:

Устройства веб-безопасности определяют чувствительную информацию, которая передается в веб-потоке во внешнюю среду: номера кредитных карт, списки клиентов, документация и другая коммерческая информация. Система имеет гибкие настройки, которые помогают автоматически определять и блокировать подобные инциденты.

Категория затрат	Описание	Затраты на 1 запись
Определение, реагирование и уведомление	Юридические затраты, уведомление клиентов, увеличение нагрузки на call center, маркетинг и PR, занижение стоимости предложения	$50
Потеря продуктивности работы сотрудников	Сотрудники отвлекаются от обыденного порядка работ, наем подрядчиков	$30
Реституция*	Компенсация ущерба пострадавших клиентов	$30
Отстроченный Ущерб	Потеря будущих возможностей бизнеса (потеря клиентов)	$98
Общая стоимость утери единицы записи		*$218*

Таким образом, утечка 5 000 клиентских записей вырастает в $1,09 млн. прямых затрат. Так, как на веб-канал, включая чат-программы и персональные почтовые ящики, припадает 55% всех информационных утечек, соответственно безопасный веб-шлюз компенсирует риск, в размере $1 090000*0,55= $599500. Можно считать $0,6 млн.
В подсчетах, для наглядности, равномерно распределим эту сумму в течение года, по $50 000 ущерба в месяц.

Стоимость владения шлюзом

Стоимость комплексов веб-безопасности состоит из стоимости аппаратного обеспечения, лицензий на активацию подсистем безопасности и подписок на обновление активированных систем безопасности.

Отказоустойчивые пары высокопроизводительных шасси, движки антивирусной безопасности, фильтрации категорий сайтов на 500 пользователей с обновлениями на 3 года обойдутся приблизительно в $ 80000.

Также, в стоимость владения устройством входит стоимость его обслуживания специалистами. Так, как система автоматизированная, обслуживание устройства будет сводиться к настройке политик безопасности и дальнейшей минимальной корректировке.

Как показывает практика, время обслуживания комплексов с гармонично настроенными политиками безопасности сводиться к 1 часу в неделю. В то время как первичная настройка введенного в эксплуатацию комплекса может занимать больше времени. В расчеты также включим затраты, которые могут возникнуть поначалу из-за дополнительной нагрузки на helpdesk и простоя пользователей.

	Освобожденное время сотрудников, политика целевого интернета	Компенсация времени простоя от вирусных эпидемий	Компенсация ущерба от информационных утечек	Стоимость системы (аппаратного обеспечения, ПО, подписок)	Обслуживание системы веб-безопасности	Чистый денежный поток
Январь	75 000	0	50000	-81000	-2000	42 000
Февраль	75 000	0	50000	0	-1000	124 000
Март	75 000	45000	50000	0	-500	169 500
Апрель	75 000	0	50000	0	-500	124 500
Май	75 000	0	50000	0	-500	124 500
Июнь	75 000	0	50000	0	-500	124 500
Июль	75 000	0	50000	0	-100	124 900
Август	75 000	0	50000	0	-100	124 900
Сентябрь	75 000	0	50000	0	-100	124 900
Октябрь	75 000	45000	50000	0	-100	169 900
Ноябрь	75 000	0	50000	0	-100	124 900
Декабрь	75 000	0	50000	0	-100	124 900

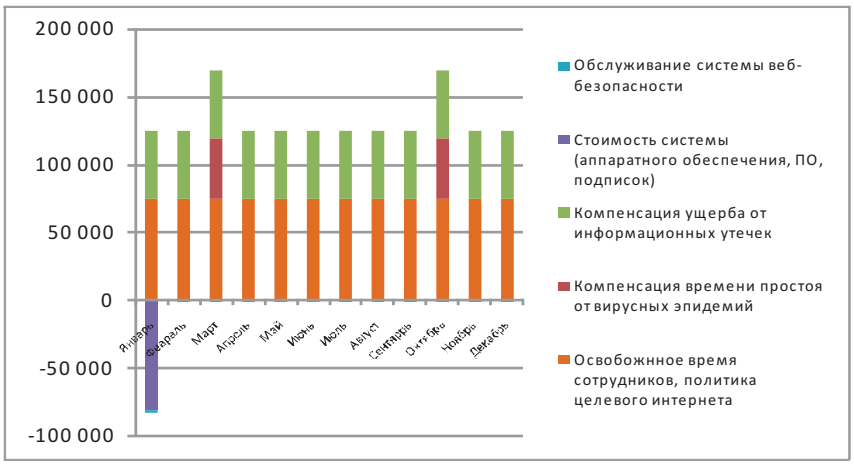


Диаграмма 2 (композитный денежный поток, полученный от инвестиций в технологию)

Итак, композитный расчет денежного потока (cash flow) показан на Диаграмме 2: Затраты на приобретение и обслуживание устройства показаны со знаком «-», возврат денег, полученных от полезной работы устройства отображены со знаком «+».

Как видно по диаграмме, окупаемость устройства происходит мгновенно. Учитывая специальную промо-стоимость комплекта из отказоустойчивых пар шасси и трехлетних подписок на 500 пользователей, компания возвращает инвестиции в технологию после первого месяца ее использования.

Даже если не учитывать риски информационных утечек и вирусной эпидемии, 100% окупаемость технологии происходит уже на втором месяц ее использования!

Качественный возврат инвестиций

Аппаратная платформа

Аппаратная платформа систем веб-безопасности – это специализированные, промышленные серверы, специально адаптированные для задач безопасности и работы под нагрузкой 24x7. Ускоренные сетевые интерфейсы, аппаратная логика коррекции ошибок и регулируемые функции самодиагностики позволяют максимально эффективно утилизировать аппаратные мощности.

Обыкновенные серверы разрабатываются для выполнения любых задач, которые заранее производителю неизвестны, поэтому их аппаратная часть будет работать медленнее с специфическими задачами, чем специально разработанное под это шасси.

+Высокая производительность

+Высокая устойчивость, класс промышленного устройства

Операционная система (ОС)

Специально архитектура операционной системы, которая разработана для задач веб-безопасности и под «собственное аппаратное шасси». Это промышленная ОС, с оптимизированным кодом и функциями самозащиты от атак. Таким образом, система работает без сбоев и исключается возможность вывести ее из строя, заразить вирусом или провести на неё атаку. Устройство устойчиво к атакам и программно-аппаратным сбоям.

Производители «общих операционных систем» заведомо не знают, какие функции она будет выполнять у каждого клиента, и на какое «железо» она будет установлена. Поэтому, эти операционные системы обладают избыточной (для нашего случая) функциональностью, и как следствие – более высокая вероятность сбоя системы. Также, для популярных видов серверных ОС разработано большое количество вирусов и атак.

+Высокая устойчивость к программным сбоям, вирусам и атакам

+Максимальная утилизация аппаратных ресурсов

Система проксирования и управления сетевыми потоками

Разработанная промышленная программа, которая оптимизирована и максимально интегрирована в собственную ОС работает без сбоев. Функции самодиагностики, самоуправления и самовосстановления удовлетворяют требованиям отказоустойчивости бизнеса BCM. Программа разработана для собственного шасси и максимально контролирует специализированные функции и возможности аппаратных контроллеров. Расширенный функционал предоставляет дополнительные функции бизнесу, например: расшифровку скрытых потоков, управление полосой пропускания, анализ нежелательного контента (веб-игры, видео, музыка).

Программные решения, которые существуют на рынке, опять-таки имеют менее оптимизированный код. Необходимый функционал у них более скромный, и требует установки дополнительных программ, что вносит сложность в систему и повышает вероятность ошибки.

+Инновационный функционал значительно шире конкурентных решений

+Оптимизированный код включает сбои программы

Потоковый антивирусный модуль и эвристический анализ кода

Интегрированный в программный «моноблок» антивирусный движок обладает повышенной производительностью, а программа анализа и разбора трафика оптимизирована для совместной работы с встроенным антивирусом. Поставщики антивирусных движков – известные производители. Также, существует возможность лицензировать несколько движков от разных производителей, выстроив эшелонированную антивирусную защиту в едином устройстве.

Антивирусные вендоры в основном сосредотачивают свои усилия на продуктах для защиты рабочих станций. Они сотрудничают с производителями многокомпонентных шлюзовых систем безопасности, разрабатывая для их систем свои движки. Тем не менее, у них есть отдельные системы, но они более дорогие, чем встроенный антивирусный движок, так как это отдельные программы со своими системами управления и модулями подключения к прокси- программам и т.д.

+Оптимизированные и интегрированные движки от известных производителей

+Возможность активировать дополнительные антивирусные движки

Система контентной фильтрации

Система веб-фильтрации оснащена дополнительными функциями контроля передаваемых типов информации, которая отсутствует у независимых разнородных продуктов. Гибкие политики управления – ограничения трафика по времени, объему, категориям, контроль пропускной полосы являются результатом синергии функций ОС, проксирующей программы и системы контентной фильтрации. Существует возможность использовать базы категорий от разных производителей.

Разнородные продукты выполняют только роль категоризации интернета и ограничивают доступ к разным категориям. Они не управляют трафиком и не создают многокритериальные политики, которые невозможны из-за того, что каждый модуль – это независимая программа.

+Гибкие функции управления трафиком, которые отсутствуют у разнородных продуктов

+Несколько баз веб-категорий

Система управления

Основные требования к управлению – это простота и эффективность (возможность тонкой настройки). Управлять множеством функций единой моноблочной системы гораздо проще, чем иметь перед собой 5 разных консолей от различных систем. Сводные отчеты, например, по пользователям (персональная статистика по трафику, вирусам, посещаемым категориям) возможна лишь в многофункциональной системе веб-безопасности

Если рассматривать решение, которое состоит из нагромождения различных приложений, мы получаем нагромождение консолей управления и отчетов из каждого отдельного приложения. Это приводит к ограниченности в настройках, некорректным настройкам и забирает много времени у администраторов.

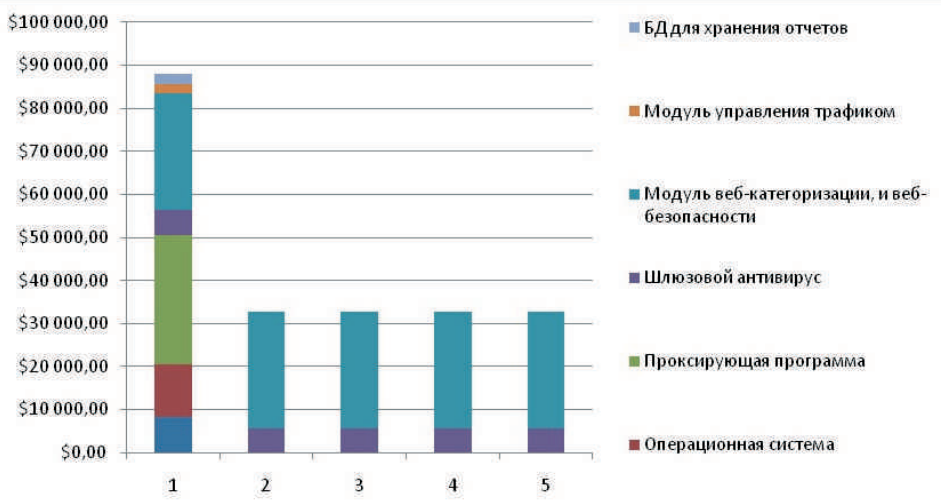
+ Сводные отчеты от множества подсистем по единому критерию

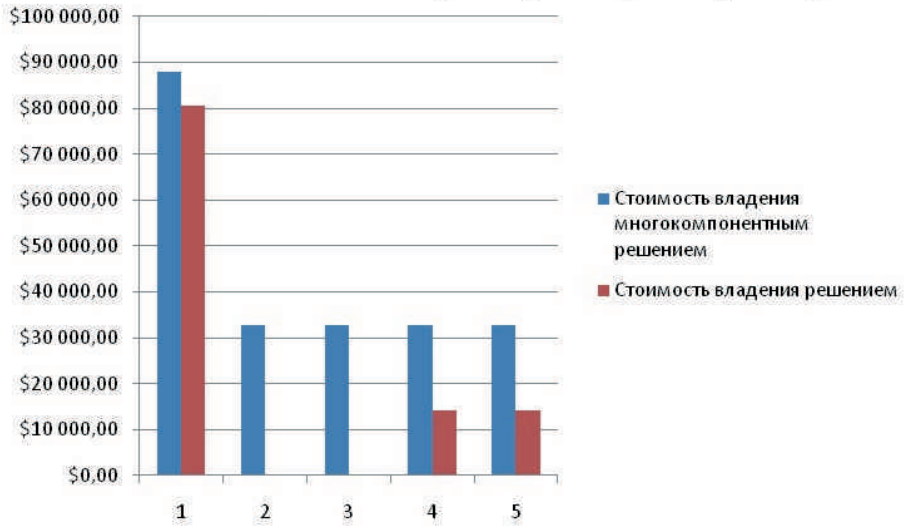
+Управления множеством подсистем из единой консоли

Экономические выгоды качественного преимущества

Давайте посчитаем стоимость владения системой в течение 5-ти лет. Цены включают НДС.

Время		1 год	2 год	3 год	4 год	5 год
Высокопроизводительные сервера	2 сервера, 2-процессорные	$8 400,00				
Операционная система	2 лицензии по 2 процессора	$12 000,00				
Проксирующая программа	2 лицензии по 2 процессора	$30 270,00				
Шлюзовой антивирус	500 пользовательских лицензий, 1 год	$5 700,00	$5 700,00	$5 700,00	$5 700,00	$5 700,00
Модуль веб-категоризации, и веб-безопасности	500 пользовательских лицензий, 1 год	$27 057,00	$27 057,00	$27 057,00	$27 057,00	$27 057,00
Модуль управления трафиком	Лицензия на сервер TMG	$2 068,00				
База данных для хранения отчетов различных программ	2 лицензии на 2 процессора	$2 400,00				
Стоимость владения решением		**$87 895,00**	**$32 757,00**	**$32 757,00**	**$32 757,00**	**$32 757,00**
Устройство веб-безопасности с поддержкой и подписками на 3 года Веб-фильтрация 500 пользователей	2 штуки - отказоустойчивый стек высокой готовности	**$80 640,00**	**$0,00**	**$0,00**	**$14 160,00**	**$14 160,00**
Устройство с поддержкой и подписками на 3 года Антивирус 500 пользователей	2 штуки - отказоустойчивый стек высокой готовности					





Кроме того внедрение систем веб-безопасности обеспечивает:

Выполнение требований BCM (Business Continuity Management)

по отказоустойчивости системы и непрерывности бизнес-процессов.

Выполнение и автоматизация требований ISO 27001, 27002

Данный стандарт вводит Национальным Банком Украины

Выполнение требований стандарта PCI-DSS для банков

Выполнение требований стандарта безопасности платежных карт. Система покрывает все возможные требования, которые относятся к веб-каналу: 7 из 12 требований.

Повышение эффективности работы компании на 25.%

Исходя из освободившегося времени у сотрудников, они больше времени будут уделять непосредственным рабочим задачам.

Повышение эффективности работы ИТ-отдела

Минимально ресурсозатратное обслуживание системы:
- централизованное управление и отчетность;
- автоматизация и интеллектуальное реагирование.

Оптимизация использования интернет-канала

Предоставление гарантированной полосы пропускания для критичных приложений и сотрудников, которым это необходимо. Высвобождение ресурсов интернет-канала после фильтрации нецелевых протоколов и веб-ресурсов.

Компания Information Systems Security Partners (ISSP) – интегратор решений по безопасности информационных систем для украинских компаний и зарубежный компаний, которые работают в Украине.

Обладая компетенциями по продуктам и обширной экспертизой в области информационной безопасности, компания ISSP обеспечивает полный спектр услуг в проектном цикле внедряемых технологий.

ООО “Информейшн Системс Секьюрити Партнерс”

03056, Киев, ул. Полевая 24
тел. +380 44 393 15 66
факс +380 44 393 15 67
e-mail info@issp.ua
web www.issp.ua