Институт информационной безопасности компании
«Инфосистемы Джет»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению практических работ по курсу

SOCостроение

Для руководителей подразделений информационной безопасности, служб экономической безопасности, экспертов по информационной безопасности

Москва
2017

Основные положения

1. Настоящие Методические указания описывают общий подход к оценке затрат на построение Центра управления инцидентами ИБ (SOC, Security Operation Center), определению количества и стоимости необходимого персонала, а также один из подходов к формированию тарифов при оказании услуг аутсорсинга SOC.
2. В качестве основного технического оснащения SOC рассматривается SIEM-платформа и не учитывается весь возможный комплекс технических средств для обнаружения атак и угроз, таких как IPS, сканер уязвимостей, UEBA, др.
3. Приведенная методика предназначена для бюджетирования расходов на построение SOC и для обоснования закупки услуг аутсорсинга.
4. Под EPS (количество событий в секунду) понимается совокупный поток данных от информационных систем и средств защиты, поступающий в SIEM для последующей корреляции и выявления событий ИБ.
5. Под событием ИБ понимается выявленное на основе срабатывания корреляционных правил SIEM состояние системы, услуги или сети, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.
6. Под инцидентом ИБ понимается подтвержденное нарушение или существенная угроза нарушения ИБ компании, выявленные по результатам анализа событий ИБ.

Автор Методических указаний:
Сюртукова Екатерина Валентиновна

Институт информационной безопасности
компании «Инфосистемы Джет»

Практическая работа №1

Определение совокупной стоимости владения SOC

Цель работы: научиться рассчитывать совокупную стоимость владения SOC с учетом капитальных и операционных затрат

Порядок расчета

1. Совокупная стоимость владения SOC (***TCO, руб.***) определяется как сумма капитальных и операционных затрат с учетом срока планирования:

   TCO на X лет = CAPEX + OPEX × X, где

   X – срок планирования, годы;

   CAPEX – капитальные затраты на старте, руб.;

   OPEX – операционные затраты в год, руб.

2. Определяем разовые капитальные затраты на старте проекта по построению SOC (***CAPEX***). Основные составляющие капитальных затрат – это техническое оснащение, работы по внедрению, настройке, процессному обеспечению:

   $CAPEX = CAPEX_{infr} + CAPEX_{impl}$, где

   $CAPEX_{infr}$ – стоимость технического оснащения, руб.;

   $CAPEX_{impl}$ – стоимость работ по внедрению, настройке, процессному обеспечению, руб.

   2.1. Оцениваем стоимость технического оснащения SOC ($CAPEX_{infr}$).

   Статьи затрат на техническое оснащение приведены в Табл.1. Стоимость каждой статьи оценивается индивидуально. Состав технических средств определяется на этапе эскизного проектирования.

Табл.1.

№	Статья затрат	Краткое описание	Оценка затрат
1.	Техническое оснащение		
1.1.	SIEM, программная платформа	Стоимость лицензий зависит от ожидаемого потока событий – EPS и дополнительных опций.	___ руб.

1.2.	Инфраструктура для SIEM-системы в отказоустойчивом исполнении	• аппаратные ресурсы HW; • среда виртуализации VM, ОС; • видеостена; • резервное копирование; • сетевое оборудование; • пр.	___ руб.
Итого:			___ руб.

2.2. Оцениваем стоимость работ на старте (***CAPEX$_{impl}$***).

Составляющие работ на старте приведены в Табл.2. Необходимо определиться, какие работы будут выполняться собственными силами, а какие с привлечением внешней компании. После этого запросить стоимость работ.

Табл.2.

№	Статья затрат	Краткое описание	Оценка затрат
1.	Работы на старте		
1.1.	Затраты на внедрение тех. средств (стоимость работ)	• обследование и проектирование; • внедрение и настройка SIEM-системы; • подключение источников; • разработка и реализация правил корреляции для сценариев выявления инцидентов.	_____ руб.
1.2.	Затраты на процессное обеспечение (стоимость работ)	• определение ключевых ролей, сроков подключения, типовых настроек; • разработка регламента расследования и реагирования на инциденты ИБ; • разработка инструкций оператора/аналитика/пользователя; • пр.	_____ руб.
Итого:			_____ руб.

3. Определяем операционные затраты (***OPEX***) на 1 год. Основные составляющие операционных затрат – продление поддержки производителя оборудования и ПО, поддержка ИТ-интегратора, затраты на штат:

$$OPEX = OPEX_{vendor} + OPEX_{support} + OPEX_{staff},$$ где

$OPEX_{vendor}$ – стоимость продления лицензий и техническая поддержка производителя, руб.;

$OPEX_{support}$ – стоимость работ по технической поддержке ИТ-интегратора: базовые консультации, восстановление работоспособности, профилактические работы, руб.;

$OPEX_{staff}$ – затраты на штат SOC, руб.

Значения $OPEX_{vendor}$ и $OPEX_{support}$ запрашиваем у соответствующего партнера/ИТ-интегратора/производителя оборудования и ПО.

3.1 Определяем затраты на штат SOC.

Для начала нужно понять, какие функции должен выполнять SOC и какие роли и компетенции для этого нужны.

Основные группы специалистов, задействованные в SOC: группа мониторинга, группа реагирования на инциденты, аналитики ИБ, администраторы SIEM, технические эксперты, руководитель SOC. Для определения совокупных затрат на персонал необходимо определить количество специалистов каждой группы и их стоимость:

$$OPEX_{staff} = C_1 \times P_1 + C_2 \times P_2 + C_3 \times P_3 + ... + C_n \times P_n,$$ где

C_n – количество специалистов каждой группы специалистов, шт.;

P_1 – средняя стоимость специалиста для компании с учетом всех составляющих, налогов, социального пакета, руб.

3.1.1. Определяем необходимое количество специалистов SOC.

Сначала нужно определить плановую трудоемкость (T) групп специалистов, занимающихся непосредственно операционной деятельностью по обработке событий ИБ, в зависимости от ожидаемой нагрузки, в человеко-днях:

$$T = t_i \times N_i,$$ где

N_i – ожидаемый поток событий ИБ, шт. в год (не путать с EPS);

t_i – среднее время обработки 1 события, человеко-дни.

Зная плановую трудоемкость каждой операционной группы, определяем количество специалистов:

C = ОКРВВЕРХ (T/(250×0.7); 1), где

250 – это количество рабочих дней в году 1 специалиста, дни;

0,7 – коэффициент, учитывающий 70% продуктивную загрузку специалистов (учитывает отпуска, болезни, время на самообразование и пр.).

Количество прочих специалистов SOC, таких как руководитель SOC, аналитик, технический эксперт, определяется индивидуально исходя из планируемой архитектуры и места команды SOC в организационно-штатной структуре компании.

Примечание:

- *Если работа группы по обработке событий ИБ должна осуществляться в режиме 24x7, а расчетное количество специалистов мониторинга получилось < 5, необходимо С принять равным 5, т.к. для составления графика сменности с учетом требований Трудового кодекса о нормативах рабочего времени специалистов круглосуточной службы оно должно быть* ***не менее 5****.*
- *Если какая-либо компетенция/роль закрывается одним специалистом, необходимо предусмотреть вариант подмены на время отпусков,* болезней, увольнения.

3.1.2. Определяем стоимость сотрудника для компании.

Оценка стоимости одного сотрудника для компании (P_1) определяется с учетом всех составляющих согласно Табл.3.

Табл.3.

Статья затрат	На одного сотрудника в месяц
Основные расходы на сотрудника	
Средняя з/п одного сотрудника в месяц (net) в руб.	A руб./год
НДФЛ, 13 %	13% от A
Взносы в пенсионный фонд, социальное страхование, ФМС, страхование от НС и ПЗ (22%, 2,9%, 5,1%, 0,5%)	30.5 % от (A+НДФЛ)

Дополнительные расходы на сотрудника	
Стоимость обучения	10% от А
Затраты на поиск персонала HR	5% от А
Организация и обслуживание рабочих мест (аренда помещения/компьютерная техника/электричество/бэк-офис и пр.)	25% от А
Премии, бонусы, оплата переработок	20% от А
Социальный пакет, ДМС и пр. (~20 000 руб. на сотрудника в год)	_____ руб./год
Итого стоимость сотрудника для компании в год:	P_1 , руб./год

Примечание: Грубую оценку можно получить умножением заработной платы сотрудника на коэффициент 2-2,5.

3.2. Учет ставки дисконтирования.

Операционные расходы рассчитываются в настоящий момент времени на долгосрочную перспективу, необходимо учитывать будущие денежные потоки по отношению к текущей стоимости денег. Для учета изменения стоимости денег во времени из-за инфляции и пр. применяется понижающий коэффициент с учетом ставки дисконтирования.

Операционные расходы с учетом снижения стоимости денег в будущем определяются как:

$$OPEX = \frac{OPEX_{1\ год}}{(1+d)^1} + \frac{OPEX_{2\ год}}{(1+d)^2} + \ldots + \frac{OPEX_{X\ год}}{(1+d)^X}$$, где

X – срок планирования, годы;

d – ставка дисконтирования в год – это процентная ставка, которая учитывает изменение стоимости денег во времени, уровень инфляции, норму доходности инвестора.

В нашем расчете при оценке OPEX ставка дисконтирования может быть применена к $OPEX_{vendor}$ (стоимости продления лицензий на последующие годы) и $OPEX_{support}$ (поддержка ИТ-интегратора) в случае, если эти суммы существенны и фиксируется на весь срок X.

При оценке $OPEX_{staff}$ ставку дисконтирования не учитываем, так как основная составляющая данной статьи операционных расходов – это заработная плата персонала, которая подлежит ежегодной индексации с учетом инфляции.

Практическая работа №2

Формирование тарифов на услуги аутсорсинга SOC

Цель работы: освоить метод формирования стоимости услуг SOC в зависимости от потока событий EPS.

Если SOC строится с целью оказания услуг дочерним предприятиям или вашим клиентам, для формирования тарифов с целью монетизации сервиса и выхода на прогнозируемую окупаемость можно применять указанный ниже подход.

Порядок расчета

1. Определяем список потенциальных клиентов и объем целевой инфраструктуры, которую необходимо будет подключить к SOC.
2. Определяем совокупные затраты на организацию и владение SOC (***TCO***) с учетом объема инфраструктуры потенциальных клиентов по методике, описанной в Практической работе №1.
   2.1. При определении ***TCO*** нужно ориентироваться на срок инвестирования не менее 3-5 лет. Меньший срок инвестирования приведет к формированию завышенных тарифов и потере конкурентоспособности.
   2.2. Для оптимизации разовых затрат целесообразно рассмотреть MSSP-схему закупки лицензий, когда оплата производится из расчета фактического потребления (Pay as You Grow).
3. Формируем тарифы на услуги и оцениваем доходную часть (рассмотрим подход на примере услуги мониторинга).
   3.1. Тарифы на услуги должны быть сформированы таким образом, чтобы при подключении целевого количества клиентов все затраты окупились в течение срока инвестирования. При этом необходимо учесть ежегодное дисконтирование денежных потоков. Дисконтированный доход на X лет рассчитывается как:

$$NPV = \sum_{t=0}^{X} \frac{CF_t}{(1+d)^t}, \text{ где}$$

d – ставка дисконтирования в год, %;

CF_t – доход через t лет, руб.

Для того чтобы учесть временную стоимость денег, при формировании тарифов нужно применять повышающий коэффициент (***K***). Допускается упрощенный его расчет по следующей формуле:

$$K=(1+d)^X$$

3.2. Стоимость услуги мониторинга формируем в зависимости от типов и количества подключаемых источников, т.к. эти параметры влияют на основные составляющие затрат – стоимость платформы SIEM и трудоемкость работ.

3.3. За основу тарификации берем базовую стоимость услуги для 1 EPS (***Z eps***). Зная перечень источников клиента и соответствующее им количество EPS (ориентировочные справочные значения – см. Табл.4), формируем итоговую стоимость услуги.

3.3.1. Определяем стоимость услуги для 1 EPS (***Z eps***). Для этого все затраты TCO с учетом повышающего коэффициента делим на расчетное количество EPS (***Z eps***), которое закладывалось в спецификации SIEM. Таким образом,

Z eps в месяц = (TCO×K / V eps) / (X×12), где

TCO – совокупная стоимость владения SOC на X лет, руб.;

X – срок инвестирования, годы;

V eps – расчетное количество EPS, которое учитывалось при формировании спецификации на SIEM, события в секунду;

K – повышающий коэффициент, учитывающий снижение стоимости денег в будущем.

3.3.2. Дополнительно учитывается норма прибыли, установленная в компании, и повышающие коэффициенты для высоких параметров SLA.

3.3.3. Оценка стоимости услуги для конкретного клиента может выглядеть следующим образом:

Табл.4.

Тип источника событий безопасности	Типовое количество EPS 1 источника	Количество источников клиента	Стоимость услуги в месяц
FW – DMZ	50	5	= 50×5× Z eps
IPS/IDS	15	2	= 15×2× Z eps
AV Server	5	3	= 5×3× Z eps
WAF	25	1	= 25×1× Z eps
DNS	15	1	= 15×1× Z eps
AD	15	1	= 15×1× Z eps

СУБД	10	4	= 10×4× Z eps
Ключевые рабочие станции	1	20	= 1×20× Z eps
Коммутаторы	1	10	= 1×10× Z eps
Итого стоимость услуги:			_____ руб./ месяц

Примечание: Приведен самый простой подход с допущениями, что TCO SOC считается сразу под весь объем клиентов и что предоставляется только услуга мониторинга. На практике построение SOC и подключение клиентов происходит постепенно, поэтому финансовая модель должна учитывать этапность и возможное распределение расходов между различными услугами.

Пример расчета по Практической работе №1

Определение совокупной стоимости владения SOC

Исходные данные:

Количество подключаемых к SIEM источников – не более 50

Типы источников: AD, серверы DHCP и DNS, ОС, сетевое оборудование, AV, FW, IDS

Количество сценариев выявления инцидентов – 30

Режим функционирования SOC – 24x7

Срок планирования – 3 года

Расчет

1. Определяем разовые капитальные затраты на старте проекта SOC (***CAPEX***):

$$CAPEX = CAPEX_{infr} + CAPEXi_{mpl} = 30 \text{ млн руб.}$$

В зависимости от выбранной платформы SIEM и от того, какие работы компания готова выполнить собственными силами, итоговое значение CAPEX может варьироваться от 10 млн до 50 млн. Для дальнейших расчетов принимаем, что капитальные затраты получились равными 30 млн руб.

2. Определяем затраты на штат SOC.

2.1 Определяем необходимое количество специалистов SOC, занимающихся непосредственно операционной деятельностью.

Начнем с групп мониторинга и реагирования. В нашем случае, на первом этапе объединим эти группы в одну и определим общую численность.

Для указанного количества источников количество событий ИБ в год (экспертная оценка, не путать с EPS) N_i = 1500-3000, среднее время обработки 1 события ИБ t_i=30 мин=0,0625 человеко-дня, плановая трудоемкость группы мониторинга и реагирования получается равной:

$T = t_i \times N_i = 3000x0,065 = 195$ человеко-дней в год.

Расчетное количество специалистов группы мониторинга и реагирования:

$$C = ОКРВВЕРХ\ (195/(250\times0.7);\ 1)=2.$$

Для режима 5x8 двух специалистов было бы достаточно, но т.к. требуется режим 24x7, принимаем C равным 5.

Экспертно определяем количество остальных специалистов SOC, получаем:

- руководитель SOC – 1 специалист;
- аналитики SOC – 1 специалист;
- технические эксперты – 1 специалист;
- администраторы SIEM – 1 специалист.

С целью оптимизации затрат не будем учитывать подмену, ограничимся минимальными цифрами и предусмотрим ночные дежурства. Возможность совмещения должностей в данном расчете не учитываем.

2.2 Определяем стоимость сотрудников для компании ($P_{(1..n)}$) с учетом всех составляющих согласно Табл.3. Расчет сделан для специалиста группы мониторинга и реагирования с заработной платой 75 000 руб. в месяц.

Статья затрат	На одного сотрудника в месяц
Оператор группы мониторинга ИБ (средняя з/п одного сотрудника в месяц, net, в руб.)	900 000 руб./год
НДФЛ (13 % от з/п net)	134 483 руб./год
Взносы в пенсионный фонд, социальное страхование, ФМС, страхование от НС и ПЗ (22%, 2,9%, 5,1%, 0,5% от з/п gross)	315 517 руб./год
Дополнительные расходы на сотрудника	
Стоимость обучения (из расчета 10% от з/п net)	90 000 руб./год
Затраты на поиск персонала HR (из расчета 5% от з/п net)	45 000 руб./год
Организация и обслуживание рабочих мест: аренда помещения, компьютерная техника, электричество, бэк-офис и пр. (из расчета 25% от з/п net)	225 000 руб./год
Премии, бонусы, оплата переработок (из расчета 20% от з/п net)	180 000 руб./год
Социальный пакет, ДМС и пр.	20 000 руб./год
Итого стоимость сотрудника для компании в год:	1 910 000 руб./год

3. По аналогии оцениваем стоимость остальных сотрудников SOC и определяем операционные затраты (OPEX) на 1 год. Для оценки взяты ориентировочные средние заработанные платы для г. Москвы.

№	Статья затрат	Краткое описание (количество специалистов)	Оценка затрат
1.	$OPEX_{vendor}$	Продление лицензий и техническая поддержка производителя (SIEM, HW, VM, ОС)	~ 4 млн руб./ год
2.	$OPEX_{support}$	Техническая поддержка интегратора (SIEM, HW, VM, ОС)	~1 млн руб./ год
3.	Штат SOC		
3.1.	Руководитель SOC	1 специалист	4 млн руб./ год
3.2.	Аналитики SOC	1 специалист	3,6 млн руб./ год
3.3.	Технические эксперты	1 специалист	2,9 млн руб./ год
3.4.	Администраторы SIEM	1 специалист	2,9 млн руб./ год
3.5.	Группа мониторинга и реагирования 24x7	5 специалистов	9,5 млн руб./ год
4.	Прочие косвенные расходы		1 млн руб./ год
Итого операционные расходы в год:			28,9 млн руб./год

$$OPEX = OPEX_{vendor} + OPEX_{support} + OPEX_{staff} = 28,9 \text{ млн руб./год}$$

4. Получив капитальные (***CAPEX***) и операционные расходы (***OPEX***), определяем совокупную стоимость владения ТСО в расчете на 3 года:

X – срок планирования, 3 года;

CAPEX = 30 млн руб.;

OPEX = 28,9 млн руб./год;

ТСО на 3 года = CAPEX + OPEX × X = 30 + 28,9 × 3 = 116,7 млн руб.

Контрольные вопросы и задания

Контрольные вопросы

1. Какие задачи вы хотите реализовать с помощью SOC?
2. Были ли у вас серьезные инциденты ИБ?
3. Сколько человек сейчас в штате ИБ?
4. Готовы ли вы к высоким капитальным затратам на старте?
5. Рассматриваете ли услуги аутсорсинга ИБ?

Задание №1 по Практической работе №1

Определение совокупной стоимости владения вашего SOC

1. **Определить совокупную стоимость владения SOC.**
   1.1. Определить границы инфраструктуры, в рамках которой планируется выявлять инциденты безопасности, состав источников событий ИБ.
   1.2. Определить режим функционирования SOC.
   1.3. Оценить TCO с учетом капитальных и операционных затрат.
2. **Запросить стоимость аутсорсинга отдельных функций, например, услуги мониторинга и реагирования, услуги администрирования SIEM, услуг экспертной поддержки.**
3. **Сопоставить стоимость своих ресурсов со стоимостью услуг аутсорсинга, выбрать наиболее экономически эффективный вариант.**

Запрос цен по п.2 Задания №1 и итоговое решение Задания №1 присылайте для проверки по адресу: security@jet.su

Задание №2 по Практической работе №2

Формирование тарифов на услуги аутсорсинга SOC

Самостоятельно сформировать тарифы на услуги SOC, используя подход, описанный в настоящих Методических указаниях.