ТОО «ПАЦИФИКА»
050008, г. Алматы, ул. Ауэзова 60
БЦ «Almaty Residence», офис 17А
БИН 080440005514

+7 (727) 355-00-11
+7 (7172) 28-00-82
info@pacifica.kz
www.pacifica.kz

ПОСТРОЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АНКЕТА СБОРА ПРЕДВАРИТЕЛЬНЫХ ДАННЫХ

Наименование организации _____

Контакты_____

1 Общие вопросы

1.1 Общее количество рабочих мест: _____

1.2. Имеется ли документация по информационной безопасности? Да Нет

1.3.Сколько сотрудников имеет выход в интернет? _____

1.4 Считаете ли Вы, что в компании есть информация, которую можно определить как «Конфиденциальная»? Да Нет

1.5 Определены ли в настоящее время политика и/или порядок реагирования на инциденты информационной безопасности? Приведите наименования соответствующих документов.

Да Нет

1.1 Эксплуатируется ли в Организации система класса Service Desk (название, версия)?

- _____

1.2 Есть ли физически изолированные или территориально-разнесенные объекты информатизации, в которых размещаются источники событий? Если есть разнесенные, какова пропускная способность каналов связи?

- _____.

1.3 Используются ли автоматизированные средства анализа защищенности? Если да, укажите производителя и версию сканера, а также количество сканируемых объектов.

- _____ (например, Nessus, 100 серверов)

ТОО «ПАЦИФИКА»
050008, г. Алматы, ул. Ауэзова 60
БЦ «Almaty Residence», офис 17А
БИН 080440005514
+7 (727) 355-00-11
+7 (7172) 28-00-82
info@pacifica.kz
www.pacifica.kz

1.4 Каково планируемое количество пользователей системы управления информационной безопасностью – СУИБ (Администраторов, Операторов)?

- _____

1.5 Подключаются ли сотрудники к почте извне? Каким образом? _____

1.6 Подключаются ли сотрудники к бизнес-приложениям извне? Каким образом? _____

1.7 Подключаются ли администраторы к системам извне? Каким образом? _____

1.8 Используются ли системы мониторинга целостности файлов на серверах? _____

1.9 Используются ли системы контроля за изменениями? _____

1.10 Имеется ли корпоративный интернет портал? Он подключен к бизнес-приложениям? _____

1.11 Использует ли руководство компании смартфоны и планшетные компьютеры в работе? _____

2 Характеристики СУИБ

№	Тип источника событий	Производитель, тип и версия ПО или оборудования, patch level	Механизм (OPSEC Syslog, SNMP, DB, VPM…)	Кол-во, штук	Примечания
1.	Межсетевые экраны, PROXI				
2.	Система обнаружения и предотвращения вторжений (IDS/IPS)				Также укажите количество оконечных устройств, контролируемых системой.
3.	Серверные операционные системы в ЦОД				События безопасности, такие как вход/выход пользователей и изменение привилегий.

ТОО «ПАЦИФИКА»
050008, г. Алматы, ул. Ауэзова 60
БЦ «Almaty Residence», офис 17А
БИН 080440005514
+7 (727) 355-00-11
+7 (7172) 28-00-82
info@pacifica.kz
www.pacifica.kz

№	Тип источника событий	Производитель, тип и версия ПО или оборудования, patch level	Механизм (OPSEC Syslog, SNMP, DB, VPM…)	Кол-во, штук	Примечания
4.	Сколько процессоров на серверах в ЦОД: Сколько ядер на серверах ЦОД:				
5.	Рабочие станции пользователей				Следует указывать только те рабочие станции, с которых события будут собираться непосредственно (критичные рабочие станции).
6.	По каким схемам работают Бизнес-приложения?				«тонкий клиент» «толстый клиент» «локально с последующей репликацией»
7.	Сетевые устройства (маршрутизаторы, коммутаторы)				События авторизации администраторов, изменения конфигурации, сообщения об ошибках и проч.
8.	Антивирусные системы				Также укажите количество оконечных устройств (серверов/рабочих станций), контролируемых системой.
9.	СУБД				Здесь учитываются события аудита доступа к самой БД. Например, для Oracle данные аудита хранятся в таблице SYS.AUD$.
10.	Сколько процессоров на серверах, где хранятся базы данных: Сколько ядер на серверах, где хранятся базы данных				

№	Тип источника событий	Производитель, тип и версия ПО или оборудования, patch level	Механизм (OPSEC Syslog, SNMP, DB, VPM…)	Кол-во, штук	Примечания
11.	Сервер VPN или удаленного доступа				События авторизации пользователей, выделение IP-адреса и проч.
12.	Система резервного копирования				Прочие устройства или приложения, которые планируется подключать к Системе, например, проприетарные приложения и информационные системы
13.	Контроль доступа в сеть (NAC)				Используется ли?
14.	Двухфакторная идентификация				Администраторов Пользователей
15.	Механизм обработки логов				Системы логирования SIEM. Хранятся ли данные с журналов (логи) в специальном отдельном месте?
16.	Системы шифрования:				Каким образом подключены удаленные офисы? шифрование каналов связи
17.	DLP система Сетевое DLP Хостовое DLP				
18.	Система контентной фильтрации				Использует ли компания Proxy для выхода в интернет?

№	Тип источника событий	Производитель, тип и версия ПО или оборудования, patch level	Механизм (OPSEC Syslog, SNMP, DB, VPM…)	Кол-во, штук	Примечания
					Использует ли компания систему очистки интернет трафика? Имеется ли фильтрация почты/антиспам?
19.	Сканирование на уязвимости		сканирование IP		Например, Nessus, MaxPatrol, Outpost24