Российская академия народного хозяйства и государственной службы
при Президенте РФ
Институт экономики, математики и информационных технологий

Школа IT-менеджмента

«Выбор средств защиты
или
Как рассказать о том, о чем нельзя рассказывать»

Северинов Д. В.

Москва 2024

ПРЕЗИДЕНТСКАЯ АКАДЕМИЯ

Введение

Цель работы:

Реализация проекта по построению единого защищенного периметра

Задачи:

- исследовать структуру и взаимосвязь информационных систем.
- проанализировать основные решения NGFW на российском рынке, определить их достоинства и недостатки.
- провести сравнительный анализ выбранных решений NGFW и выбрать оптимальный вариант для внедрения в информационную систему.
- разработать проектную документацию по внедрению выбранного решения.
- Провести внедрение системы NGFW после
- Разработать и настроить инструменты для автоматизации процессов NGFW

Объект исследования - ???

Знакомая карта?

ПРЕЗИДЕНТСКАЯ АКАДЕМИЯ

Об объекте защиты

Холдинг «Крона» - логистика и экспорт зерновой продукции.

ПРЕЗИДЕНТСКАЯ АКАДЕМИЯ

NGFW - Сервис защиты от сетевых угроз.

Защита периметра корпоративной сети в распределенной ИТ инфраструктуре Холдинга и филиалов реализована разными средствами с разной эффективностью.

Next Generation Firewall (NGFW, Межсетевой экран следующего поколения) обеспечивает высокий уровень защиты от угроз для сетей любого формата и размера благодаря максимальной видимости событий безопасности.

Основные функции:

- Централизованно управлять сетевой конфигурацией организации.
- Обеспечить безопасное удаленное подключение сотрудников.
- Защитить от атак веб-сайты и порталы организации.
- Выявлять и блокировать атаки, вредоносное ПО и другие угрозы.
- Осуществлять контроль приложений на рабочих станциях сотрудников.
- Предотвращать вторжения и отслеживать всю поверхности атаки.

Максимальная видимость событий безопасности

Обнаружение скрытых атак на IT-инфраструктуру и своевременная реакция на них

Использование функций безопасности

Увеличение арсенала защиты сети за счет встроенных и дополнительных функций безопасности

Различные режимы работы

Доступен выбор режима работы и набора функций для вашего устройства UserGate Next Generation Firewall (NGFW)

Способы интеграции

Различные способы интеграции позволяют подобрать подходящий формат для вашей IT-инфраструктуры

МАИ ?

Метод анализа иерархий (МАИ)

Разработан американским математиком Томасом Саати.

- Не предлагается правильного решения;
- Структурирование характеристик объектов;
- Сравнение и качественная оценка;
- Синтез приоритетов на иерархии главной цели.

Особенность метода заключается в том, что он позволяет найти вариант (альтернативу), который согласуется с пониманием сути проблемы и требованиями к ее решению.

Критерии определяются экспертом!!!

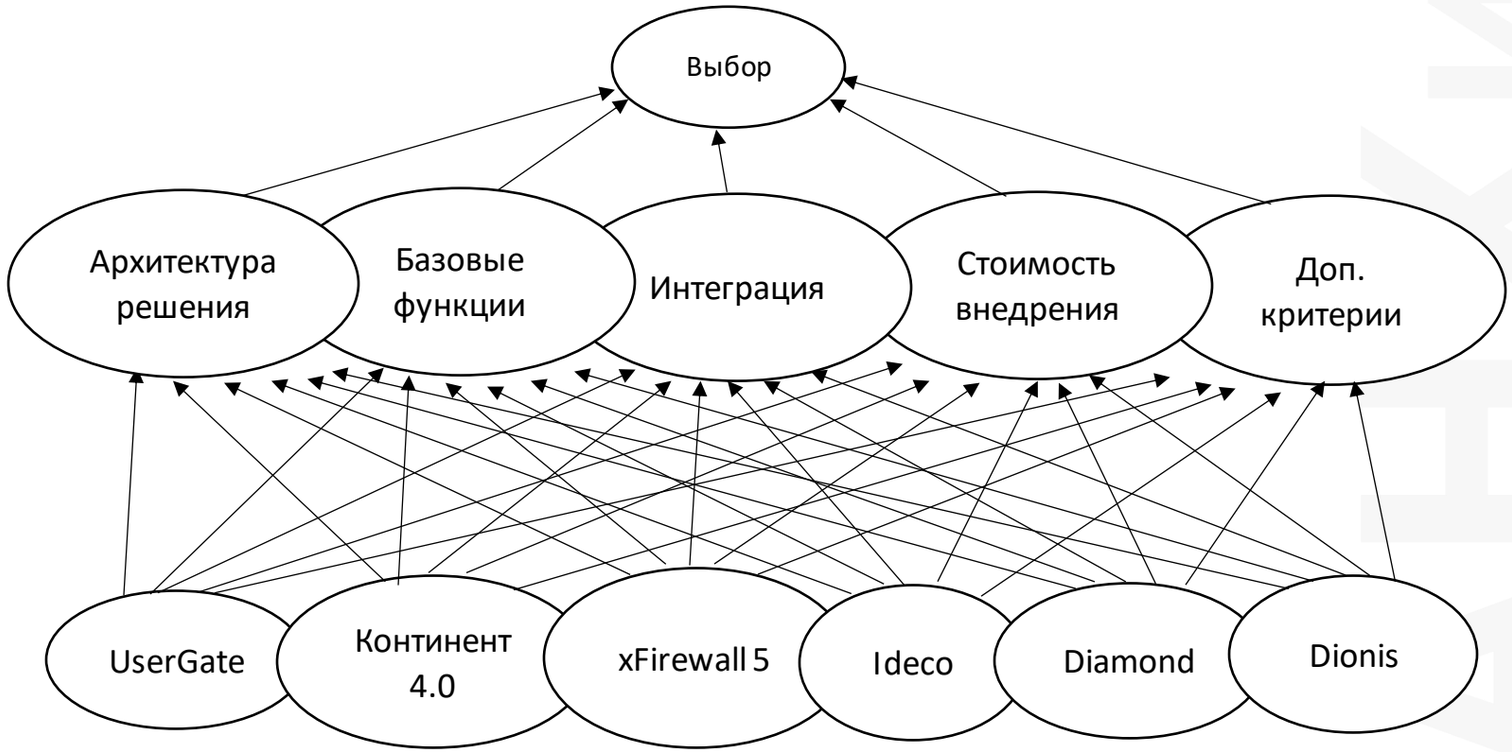
Выбор NGFW

Критерии выбора средства решения для защиты периметра сети

- Архитектура решения (К1):
- Базовые функции (К2):
- Интеграционные возможности (К3)
- Стоимость внедрения решения (К4)
- Дополнительные требования (К5)

Шкала	Значение
1	А и В важны в одинаковой мере
3	А незначительно важнее, чем В
5	А значительно важнее В
7	А явно важнее В
9	А по своей значительности абсолютно превосходит В
2, 4, 6, 8	2, 4, 6, 8 Промежуточные значения.

Подход к выбору



ПРЕЗИДЕНТСКАЯ АКАДЕМИЯ

Выбор NGFW

Критерии выбора средства решения для защиты периметра сети

Базовые значения индексов значимости для критерия «Архитектура решения»

	ViPNet xFirewall 5	Ideco NGFW	МКСЗ «Diamond VPN/FW»	ПАК Dionis DPS	UserGate (версия 6.0)	Оценки компонент собственного вектора	Нормализованные оценки вектора приоритета
ViPNet xFirewall 5	1,00	0,25	0,16	0,14	0,11	0,21	0,02
Ideco NGFW	4,00	1,00	1,11	0,20	0,14	0,54	0,06
МКСЗ «Diamond VPN/FW»	6,00	0,86	1,00	0,50	0,20	0,74	0,08
ПАК Dionis DPS	7,00	5,00	2,00	1,00	0,33	1,50	0,17
UserGate (версия 6.0)	9,00	7,00	5,00	3,00	1,00	3,83	0,43
Код безопасности Континент 4.0	7,00	5,00	3,00	2,00	0,30	1,99	0,23
Сумма коэф.	34,00	19,11	12,27	6,84	2,08	8,82	

							Сумма Lmax
Произведение суммы и нормализованной оценки приоритета	0,81	1,17	1,03	1,17	0,90	1,24	6,33

Базовые значения индексов значимости для критерия «Базовые функции»

	ViPNet xFirewall 5	Ideco NGFW	МКСЗ «Diamond VPN/FW»	ПАК Dionis DPS	UserGate (версия 6.0)	Оценки компонент собственного вектора	Нормализованные оценки вектора приоритета
ViPNet xFirewall 5	1,00	0,25	0,11	0,20	0,14	0,14	0,22
Ideco NGFW	4,00	1,00	0,14	0,33	0,20	0,20	0,44
МКСЗ «Diamond VPN/FW»	9,00	7,00	1,00	2,00	1,25	1,25	2,41
ПАК Dionis DPS	5,00	3,00	0,50	1,00	0,83	0,83	1,31
UserGate (версия 6.0)	7,00	5,00	0,80	1,20	1,00	1,00	1,80
Код безопасности Континент 4.0	7,00	5,00	0,80	1,20	1,00	1,00	1,80
Сумма коэф.	33,00	21,25	3,35	5,93	4,42	7,98	

							Сумма Lmax
Произведение суммы и нормализованной оценки приоритета	0,90	1,18	1,01	0,98	1,00	1,00	6,06

Базовые значения индексов значимости для критерия «Интеграция»

	ViPNet xFirewall 5	Ideco NGFW	МКСЗ «Diamond VPN/FW»	ПАК Dionis DPS	UserGate (версия 6.0)	Оценки компонент собственного вектора	Нормализованные оценки вектора приоритета
ViPNet xFirewall 5	1,00	0,25	0,11	0,20	0,14	0,14	0,22
Ideco NGFW	4,00	1,00	0,14	0,33	0,20	0,20	0,44
МКСЗ «Diamond VPN/FW»	9,00	7,00	1,00	2,00	1,25	1,25	2,41
ПАК Dionis DPS	5,00	3,00	0,50	1,00	0,83	0,83	1,31
UserGate (версия 6.0)	7,00	5,00	0,80	1,20	1,00	1,00	1,80
Код безопасности Континент 4.0	7,00	5,00	0,80	1,20	1,00	1,00	1,80
Сумма коэф.	33,00	21,25	3,35	5,93	4,42	7,98	

							Сумма Lmax
Произведение суммы и нормализованной оценки приоритета	0,90	1,18	1,01	0,98	1,00	1,00	6,06

Выбор NGFW

Критерии выбора средства решения

Базовые значения индексов значимости для критерия «Стоимость внедрения решения»

	ViPNet xFirewall 5	Ideco NGFW	МКСЗ «Diamond VPN/FW»	ПАК Dionis DPS	UserGate (версия 6.0)	Оценки компонент собственного вектора	Нормализованные оценки вектора приоритета
ViPNet xFirewall 5	1,00	0,33	0,13	0,13	0,11	0,11	0,20
Ideco NGFW	3,00	1,00	0,50	0,50	0,20	0,20	0,56
МКСЗ «Diamond VPN/FW»	8,00	2,00	1,00	1,00	0,83	0,83	1,49
ПАК Dionis DPS	8,00	2,00	1,00	1,00	0,71	0,71	1,42
UserGate (версия 6.0)	9,00	5,00	1,20	1,40	1,00	1,00	2,06
Код безопасности Континент 4.0	9,00	5,00	1,20	1,40	1,00	1,00	2,06
Сумма коэф.	38,00	15,33	5,03	5,43	3,85	7,78	

							Сумма Lmax
Произведение суммы и нормализованной оценки приоритета	0,97	1,10	0,96	0,99	1,02	1,02	6,06

Базовые значения индексов значимости для критерия «Дополнительные требования»

	ViPNet xFirewall 5	Ideco NGFW	МКСЗ «Diamond VPN/FW»	ПАК Dionis DPS	UserGate (версия 6.0)	Оценки компонент собственного вектора	Нормализованные оценки вектора приоритета
ViPNet xFirewall 5	1,00	0,25	0,25	0,25	0,14	0,14	0,26
Ideco NGFW	4,00	1,00	0,50	0,50	0,20	0,20	0,58
МКСЗ «Diamond VPN/FW»	4,00	2,00	1,00	1,00	0,33	0,33	0,98
ПАК Dionis DPS	4,00	2,00	1,00	1,00	0,33	0,33	0,98
UserGate (версия 6.0)	7,00	5,00	3,00	3,00	1,00	1,00	2,61
Код безопасности Континент 4.0	7,00	5,00	3,00	3,00	1,00	1,00	2,61
Сумма коэф.	27,00	15,25	8,75	8,75	3,00	8,02	

							Сумма Lmax
Произведение суммы и нормализованной оценки приоритета	0,87	1,11	1,07	1,07	0,98	0,98	6,07

Матрица векторов приоритета

Альтернативы решений систем защиты периметра	Архитектура решения	Базовые функции	Интеграционные возможности	Стоимость внедрения решения	Дополнительные критерии	Итоговые приоритеты
	Численное значение приоритета					
	0,0432	0,0755	0,1544	0,3143	0,4126	
ViPNet xFirewall 5	0,0239	0,0273	0,0273	0,0256	0,0324	0,0287
Ideco NGFW	0,0612	0,0553	0,0553	0,0717	0,0730	0,0680
МКСЗ «Diamond VPN/FW»	0,0844	0,3023	0,3023	0,1918	0,1219	0,1837
ПАК Dionis DPS	0,1704	0,1648	0,1648	0,1821	0,1219	0,1528
UserGate (версия 6.0)	0,4340	0,2251	0,2251	0,2644	0,3254	0,2879
Код безопасности Континент 4.0	0,2261	0,2251	0,2251	0,2644	0,3254	0,2789

Итоговый рейтинг выбора решения NGFW:

Производитель	Значение показателя итогового приоритета	Место в рейтинге
UserGate (версия 6.0)	0,2879	1
ПАК Dionis DPS	0,2789	2
ViPNet xFirewall 5	0,1837	3
Ideco NGFW	0,1528	4
МКСЗ «Diamond VPN/FW»	0,0680	5
Код безопасности Континент 4.0	0,0287	6

ПРЕЗИДЕНТСКАЯ АКАДЕМИЯ

Спасибо за внимание