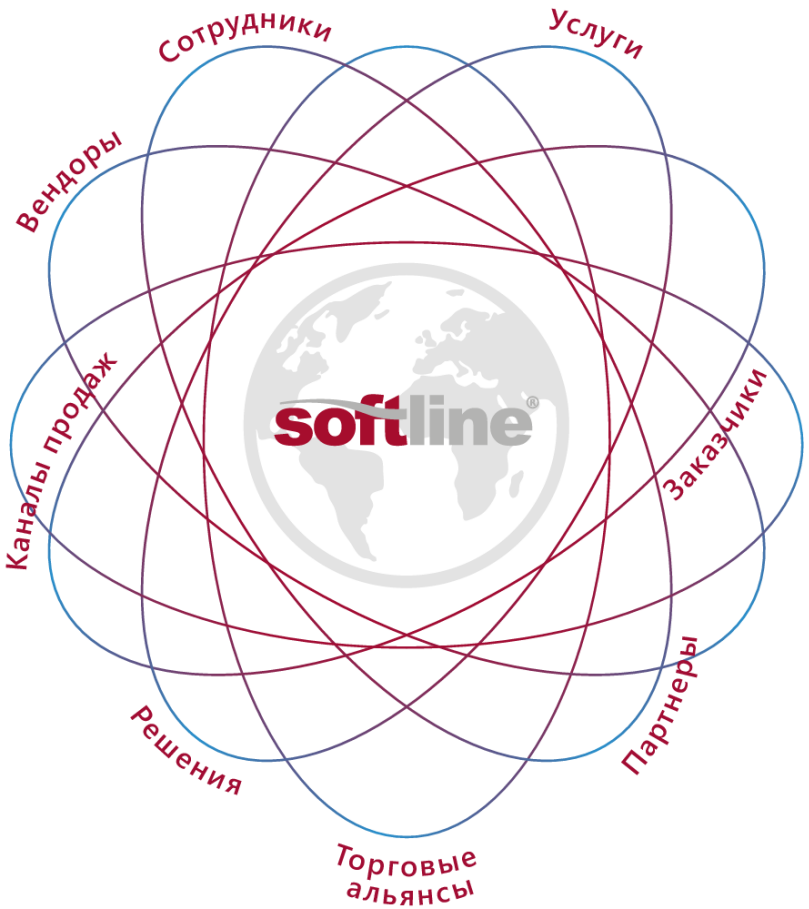
NGFW: Основные ингредиенты

Китаева Мария Сергеевна

Бизнес-консультант по информационной безопасности
Softline Волга

Лидер в цифровой трансформации и информационной безопасности



> 5 тыс.
Вендоров

> 100 тыс.
Клиентов B2B

Полный набор
Услуг и решений для цифровой трансформации

> 25
Представительств по всей России

30
Лет на ИТ-рынке

70 690 млн руб.
Оборот 2022

> 7700
Сотрудников

Цифровая Трансформация. Успешная. Эффективная.

softline SOFL

Доверенный консультант для 100 тыс. клиентов B2B

Глобальные предприятия

PEPSICO, HYUNDAI, SAMSUNG, Nestlé, Allianz, CATERPILLAR, РОСБАНК, Райффайзенбанк, P&G, TOYOTA, BAT

Крупные корпоративные клиенты

Ростех, ВГТРК, sanofi, KFC, РОСАТОМ, ИНТЕР РАО, cencosud, МЕСО, МТС, РКЦ Прогресс, KAMAZ, X5Group, Ростелеком, МегаФон, билайн, TELE2, РЖД, LEROY MERLIN, УРАЛСИБ, СБЕР, Альфа-Банк, HOME CREDIT BANK, НЛМК, Ренессанс Кредит, ВТБ, АЛЬФА СТРАХОВАНИЕ, НОВАТЭК, ТМК ТАГМЕТ, ЛУКОЙЛ, ЗАРУБЕЖНЕФТЬ, Мосэнерго, СОГАЗ, ОСК, Транснефть, РусГидро, РУСАЛ, ГАЗПРОМБАНК, РОСНЕФТЬ, МАГНИТ, QGMI, М.ВидеоЭльдорадо, ANAGI CONSTRUCTION COMPANY, СИБУР, АВТОВАЗ, АЭРОФЛОТ Российские авиалинии, ПОЧТА РОССИИ

Малый и средний бизнес

Mafatlal, ashirvad, Prestige, АГРО-ИНВЕСТ, 220 ВОЛЬТ, Geologix, CarPrice, кувалда.ру, GOLDEN GATE, FASHION COMPANY, adjarabet, ahlers, BS lab, gwp, novex, vizor LABS, heedbook

Государственный сектор

ФАС России, Sociedad de Seguros de Vida del Magisterio Nacional, ДЕПАРТАМЕНТ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ПОЖАРНОЙ БЕЗОПАСНОСТИ ГОРОДА МОСКВЫ, CAIXA

Образование и здравоохранение

MEDEM, Уральский федеральный университет имени первого Президента России Б.Н.Ельцина, ФГБУ НИИ ОНКОЛОГИИ, РОССИЙСКАЯ АКАДЕМИЯ МЕДИЦИНСКИХ НАУК, КВАНТОРИУМ, ИнтерЛабСервис, ALIBRA SCHOOL since 2000

Цифровая Трансформация. Успешная. Эффективная.

softline

Сотрудничество с 5000 вендорами

Информационная безопасность

kaspersky
positive technologies
КОД безопасности
CLOUDFLARE
RUSIEM
Стахановец
INFOWATCH
CHECK POINT
UserGate
F.A.C.C.T.
infotecs
КРИПТОПРО
Avanpost
Dr.WEB
SMART-SOFT
ПРОВЕРЕНО. БЕЗОПАСНО
с•терра
MFLASH

Облака и Виртуализация

softline облако
VK Cloud
Yandex Cloud
Kaiten
Space
КИБЕР ПРОТЕКТ
BASIS
ROS ПЛАТФОРМА
Я 360
HOSTVM
ORION SOFT
ФЛАНТ

Программное и аппаратное обеспечение

МойОфис
Р7-ОФИС
Truконф
ИНФЕРИТ
COMMUNIGATE SYSTEMS
base alt
PostgresPro
DEPO [computers]
AQUARIUS
скала^р
АСТРА группа компаний
ГРАВИТОН
GAGARIN
АЭРОДИСК мы делаем будущее
РЕДСОФТ
нанософт
ELTEX
Microsoft
ICL
HUAWEI
inspur
iru
NERPA by OCS Distribution
PANTUM
парус электро
QTECH МИР ДОСТУПНЕЕ
rocket.chat
Système electric
АСКОН
КАТЮША

Цифровая Трансформация. Успешная. Эффективная.

softline SOFL

Направления Softline

- Цифровая трансформация
- Кибер-безопасность
- Облачные решения
- Интернет вещей
- RPA
- Big Data
- Искусственный интеллект
- Программное обеспечение
- Аппаратное обеспечение
- Решения Microsoft
- Бизнес-решения: CRM, SAP, BI, документооборот
- Техническая поддержка и аутсорсинг
- Корпоративная мобильность
- Обучение и сертификация
- Управление активами, DITO
- Инженерные решения
- САПР и ГИС
- Лизинг и финансирование

ИБ в ГК Softline

ДИБ Softline — специализированная структура в компании Softline, отвечающая за развитие направления ИБ

Infosecurity — специализированный **сервис-провайдер**, оказывающий услуги в сфере информационной безопасности, IT и консалтинга

ТЦ Инженер — это команда сертифицированных экспертов, обладающие уникальным проектным опытом в консалтинге ИБ и построения СМИБ

Softline Education— Учебный центр Softline

Академия Айти — основана в 1995 году и является одним из ведущих учебно-консалтинговых центров в России и странах СНГ

Axoft — глобальный эксперт в области дистрибуции информационных технологий и сервисов — работает на IT-рынке с 2004 года

Стахановец — разработчик одноименной системы для комплексной защиты компаний от угроз информационной безопасности, предотвращения утечек данных и анализа эффективности работы сотрудников

Самые частые запросы:

- Средства межсетевого экранирования (Next Generation Firewall – NGFW)
- Криптошлюзы

Производители средств защиты информации:

КОД БЕЗОПАСНОСТИ

UserGate

ideco

SMART-SOFT®

Check Point
SOFTWARE TECHNOLOGIES LTD.

infotecs®

КРИПТОПРО

s•terra

Бизнес-задачи при выборе NGFW

Классические запросы:

- «Выпустить пользователей в Интернет»
- «Опубликовать ресурсы наружу»
- «Глубокая фильтрация трафика»
- «Защита периметра»

Неочевидные требования:

- Межфилиальный VPN (IPsec туннели): Поддержка IKEv2 - *цепляться на другое сетевое оборудование (Cisco, Eltex, Check Point и др.)*
- Пользовательский VPN (*удаленное подключение с личных или доменных устройств*)

Нюансы при выборе

Межфилиальный VPN (IPsec туннели)

Поддержка IKEv2 – *при задаче цеплять туннели на другое сетевое оборудование (Cisco, Eltex, Check Point и др.)*

К примеру:
- у UserGate IKEv2 появился только в версии 7.1, а в популярной версии 6.9 его нет – результатом следует падение и непрогнозируемое поведение туннелей, простои продуктивного контура.

- Континент 4 на текущий момент пока НЕ имеет поддержки IKEv2, работает в связке «Континент4 филиал 1 - Континент4 филиал 2».

для справки…у криптошлюзов с ГОСТшифрованием такой проблемы нет…
т.к. работают только в своей экосистеме.

Пользовательский VPN (удаленное подключение с личных или доменных устройств)

- *Не у всех NGFW есть клиентское VPN-приложение*

- Не все клиентские VPN-приложения поддерживают большинство ОС.

К примеру:
- У UG клиентское приложение официально опубликовано на сайте, но пока не доступно к коммерческой продаже. Находится в стадии B-тестирования. Поддерживаться будет: Win – в процессе устранения юридических нюансов с MS. Linux – дистрибутив в разработке.

- Континент ZTN – доступен в Appstore, доступен под Mac, iOS, Аврора, Win, Linux.

Оказываемые услуги и сервисы:

1. Демонстрация продуктовых решений

2. Пилотное тестирование:

Практическая проверка функциональных возможностей и требований к решению

3. Внедрение средств защиты информации:

Предпроектное обследование, техническое проектирование (разработка документации), пусконаладочные работы (монтаж, установка и настройка), опытная эксплуатация и приёмо-сдаточные испытания

4. Рекуррентные сервисы:

Техническая поддержка и сопровождение

Управляемые услуги (Managed Security Services, MSS’P)

5. Выделенные и разовые услуги по запросу

Команда Производства

В составе команды Сетевая безопасность по фокусным Вендорам обучены:

- 1 Старший архитектор
- 3 Архитектора
- 5 Ведущих инженеров
- 4 Инженера
- 4 профильных Руководителя проектов

Поддерживаются компетенции по UserGate, Check Point, Код Безопасности, КриптоПро, ИнфоТеКС, S-Terra, Ideco, Smart-Soft и др. (по запросу)

Демонстрация решения и пилотное тестирование

Подтверждение возможности для решения бизнес-задач Заказчика

Демонстрация решения:

- Уточнение функциональных требований к решению
- Наличие подготовленных внутренних демостендов
- Подключение технического специалиста для целенаправленной демонстрации и ответов на возникающие у Заказчика вопросы

Пилотное тестирование:

- Практическая проверка функциональных возможностей и требований к решению в пилотной зоне тестирования
- Подготовка Устава пилотного проекта и Программы и методики испытаний
- Разработка детализированного отчёта по результатам тестирования
- Выдача рекомендаций по покрытию векторов угроз
- Демонстрация функциональных возможностей
- Качественный переход и реализация Проекта по внедрению

Внедрение средств защиты информации

Организация систем информационной безопасности на базе продуктовых решений ЦК Сетевая безопасность

Выполняемые работы по этапам:

- **Предпроектное обследование:** обследование инфраструктуры, проектирование целевой архитектуры внедрения системы, актуализация сетевых схем
- **Техническое проектирование (разработка документации):** разработка и согласование с Заказчиком комплекта документации в соответствии с требованиями к техническому проекту
- **Монтажные/инсталляционные работы:** установка и преднастройка программных, программно-аппаратных и технических средств организуемой системы
- **Пусконаладочные работы:** настройка программных, программно-аппаратных и технических средств организуемой системы в соответствии с техническим проектом
- **Опытная эксплуатация и приёмо-сдаточные испытания:** проведение донастройки системы по результатам опытной эксплуатации и прохождение приёмо-сдаточных испытаний в соответствии с программой и методикой испытаний

Техническая поддержка и сопровождение систем ИБ

Сопровождение эксплуатации и функционирования системы Заказчика профильными специалистами

Базовая ТП	• Регистрация и ведение заявок • Передача информации/логов в поддержку Производителя и отслеживание статуса
Стандартная ТП (консультационная)	• Базовая ТП + консультационные услуги по функционалу, настройке и восстановлению работоспособности
Расширенная ТП (инцидентная)	• Стандартная ТП + подключение эксперта к решению инцидентов

Выделенные и разовые услуги: Комплексный аудит безопасности инфраструктуры

Аудит настроек безопасности инфраструктуры и её компонентов с точки зрения безопасности и на соответствие лучшим практикам, рекомендациям Производителей, мировым стандартам

Аудит настроек безопасности

- AD
- Контроллеры домена
- Терминальные фермы
- Настройки безопасности серверов и АРМ
- Системы защиты почты

Анализ конфигураций

- Сетевого оборудования L2-L3
- IP-телефония
- WI-FI
- NGFW
- Схем сети

Комплексный аудит безопасности инфраструктуры

Примеры отчетов

3. ПРОВЕДЕННЫЕ РАБОТЫ

3.1. Административные мероприятия

3.1.1. Деавторизация сотрудника в Подрядчиках телеком-усл

Для мини
каналы управлени
– услуги D
– телеком
– центры
– иные об

3.1.1.1. Услуги

DNS-зоны
CENTER (АО «Ре
В качестве
для блокировки не
В качестве

3.3.4.2. Рабочие станции

Для смены пароля УЗ локального администратор
проведения работ недоступными, а также для системати
PowerShell-скрипты, запускаемые с общедоступного с
политик **Export LocalAdmins**, **Set Server LocalAdmin Pa**

Групповая политика **Export LocalAdmins** назнач
группе **Компьютеры домена**.

Групповая политика **Set Server LocalAdmin Pass**
Servers[redacted] применяется к группе **Компью**

Групповая политика **Set Workstation Loca**
OU=[redacted] применяется к группе **К**

Список PowerShell-скриптов приведен в табл. 7.

СКРИПТ	
[redacted]NETLOGON\scr\ExportLocalUsersAndGroups.ps1 (MD5 bb72292611b30d101954bfb0dd3cf336)	Выгрузка
[redacted]NETLOGON\scr\setuppas_arm.ps1 (MD5 3441e34f889a2d83a52722b7e5d48959)	Смена па рабочих
[redacted]NETLOGON\scr\setuppas.ps1 (MD5 663ee626253017dec9cf4980584d4b05)	Смена па рабочих

Краткое общее Заключение для Руководителя.

Ниже представлен список обнаруженных проблем, влияние и способы их решения и/или минимизации рисков

. Недостаточный уровень документирования объектов инфраструктуры:

- информация разрознена и не структурирована. Отсутствуют версионность документов и их авторы.
- Сетевые схемы изображены без необходимых элементов (адреса управляющих интерфейсов) и уровней (от trunk)
- Нет актуальных фотографий оборудования (сервера, активное сетевое оборудование, СХД)

Влияние:

Предлага

5. РЕКОМЕНДАЦИИ

Рекомендации по устранению угроз, выявленных в IT-инфраструктуре Заказчика, приведены в табл. 12.

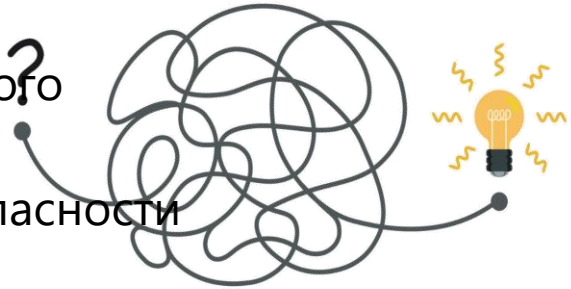
Таблица 12. Рекомендации по устранению угроз

ТИП ЭЛЕМЕНТА ИНФРАСТРУКТУРЫ	ТИП	ЭЛЕМЕНТ ИНФРАСТРУКТУРЫ	ОПИСАНИЕ УГРОЗЫ	УГРОЗА	ОЦЕНКА КРИТИЧНОСТИ ПО ШКАЛЕ RYG[A]	УСТРАНЕНИЕ	КОМПЕНСИРУЮЩИЕ МЕРЫ
Сеть	Удаленный доступ	VPN-серверы	Множественные точки подключения к сетевому периметру организации для обеспечения удаленного доступа	Отсутствие единой точки контроля по подключению к сетевому периметру организации не дает возможности оперативно блокировать нарушителя и сформировать отчет об активных подключениях		Обеспечить единую точку подключения к сетевому периметру организации для пользователей. Для технического персонала обеспечить альтернативное подключение для диагностики и исправления IT-инфраструктуры, использующееся в исключительных случаях	
			Множественные точки подключения к сетевому периметру организации для обеспечения	Отсутствие единой точки контроля по подключению к сетевому периметру			

Решение индивидуальных задач по запросу

Варианты дополнительно предоставляемых услуг

- Обновление версий прикладного ПО сетевых средств защиты информации
- Настройка и внесение изменений в политики и конфигурацию средств межсетевого экранирования
- Горизонтальное масштабирование используемых систем информационной безопасности
- Разработка пользовательских правил по анализу трафика



- *… и другие работы по модернизации инфраструктуры, рекомендованные по результатам аудита*

softline®

Цифровая Трансформация.
Успешная. Эффективная.