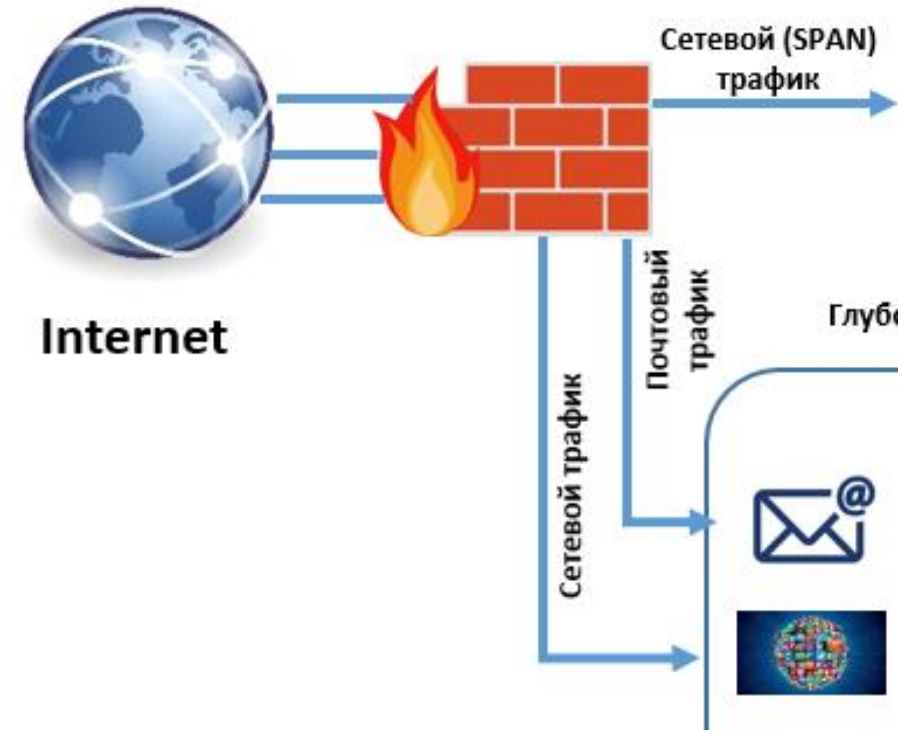
«Развитие навыков специалистов ИБ в рамках импортозамещения»

Гуревич Алексей
РГ «Кибербезопасность»
НТИ «Энерджинет»

Объем рынка NGFW в Российской Федерации



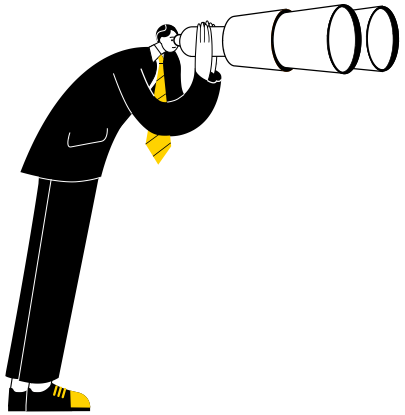
*Объем российского рынка многофункциональных межсетевых экранов (NGFW) в 2025 г. достигнет 30 млрд руб.

Ежегодный рост в данном сегменте (с 2022 года) - 15%

Количество представленных вендоров:
30 - 40 вариантов решений.

https://www.comnews.ru/content/233142/2024-05-15/2024-w20/1008/rossiyskom-rynke-ngfw-vyzhivut-ne-vse

Стоп критерии при рассмотрении МЭ (импортозамещение)



Наличие представительства или партнерской сети в РФ и поддержки на территории РФ

Подтвержденные проекты внедрения в РФ в предметной области ПС

Локализация ПО (русский интерфейс)

Платформа должна иметь дорожную карту развития (не содержать планов по снятию с поддержки)

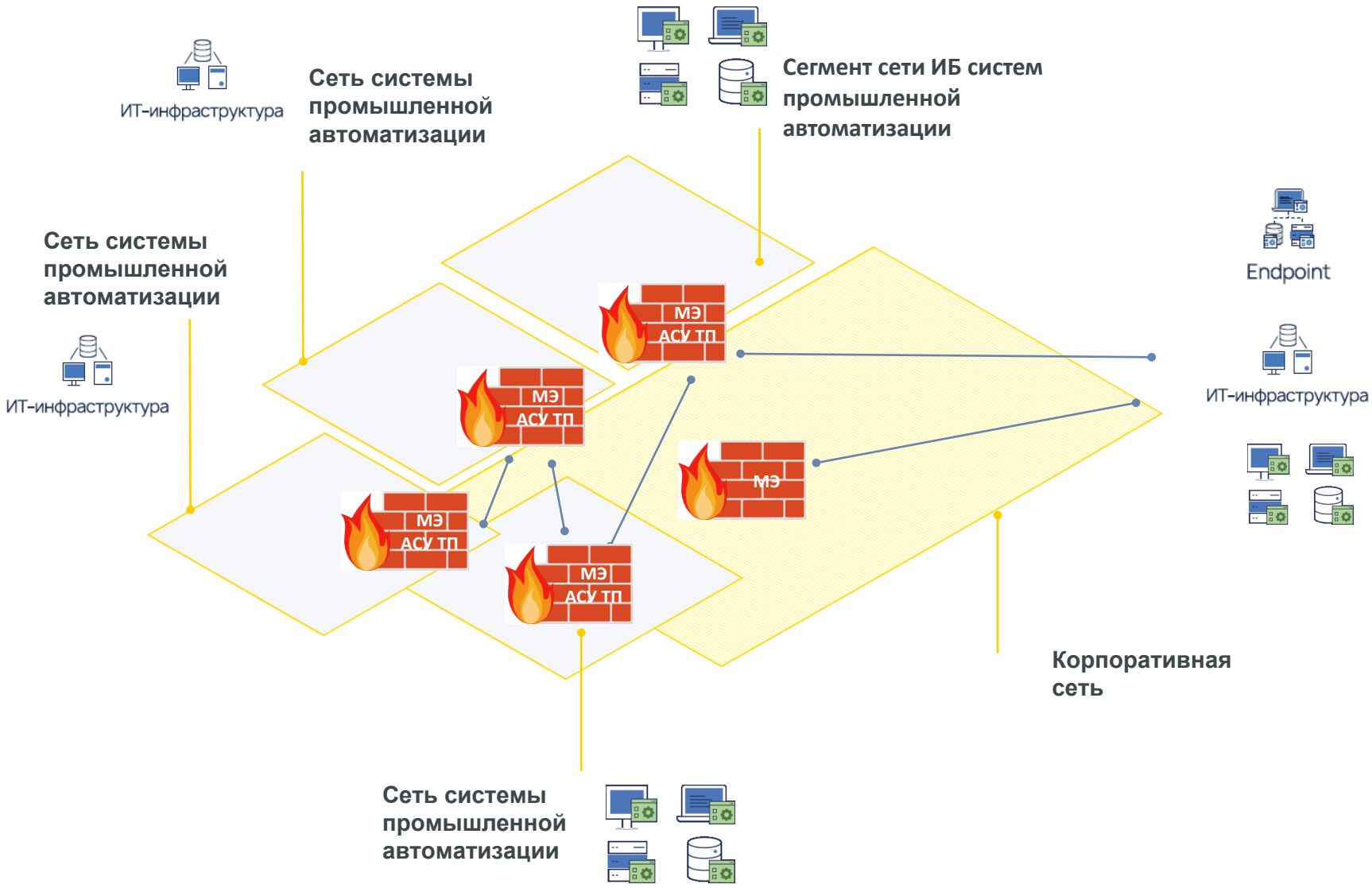
Отказ в сотрудничестве с российскими компаниями в связи с санкционными рисками

Базовая функциональность

Использование технологии публичных/гибридных облачных вычислений для обработки конфиденциальной информации

Обоснованные требования ИБ (в части рисков ИБ: наличие информации о серьезных уязвимостях, закладках в продукте и пр.), а также рисков утечки конфиденциальной информации: наличие информации о неконтролируемых потенциальных каналах утечки и пр.

Тестирование NGFW



Тестирование NGFW

Основные несоответствия рассматриваемых платформ требованиям ИБ, неустранимые применением дополнительных СЗИ:

МЭ, вендор 1:

- УПД.1 (отсутствует возможность создавать новых пользователей, перечень пользователей жёстко задан производителем, имеется только возможность смены пароля)

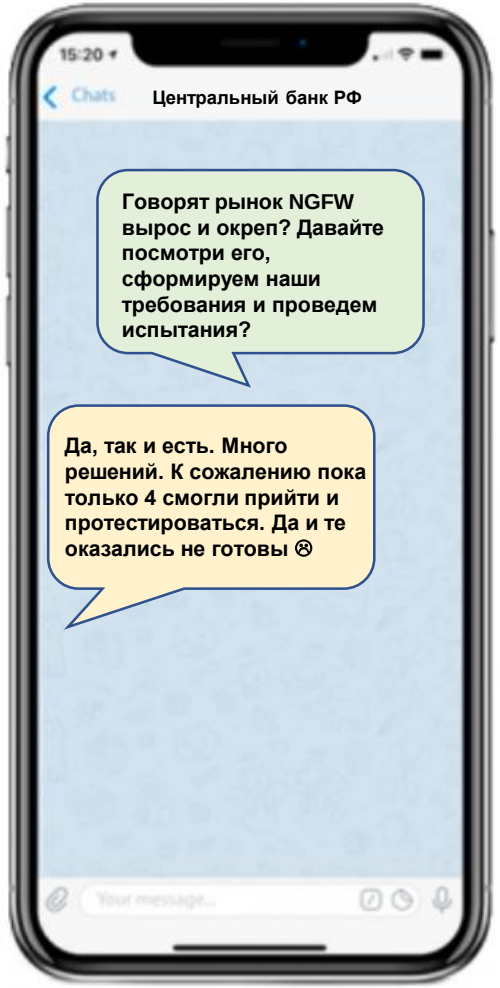
МЭ, вендор 2:

- УПД.3 (не обеспечивается доверенная загрузка)
- УПД.10 (не обеспечивается блокирования сеанса пользователя при неактивности)
- ЗНИ.7 (не осуществляется контроль внешних носителей)
- УПД.10 (не обеспечивается блокирования сеанса пользователя при неактивности) - Management Center

МЭ, вендор 3:

- УПД.10 (сеанс пользователя блокируется при неактивности не на всех страницах веб интерфейса InfoWatch ARMA Industrial Firewall)
- УПД.10 (сеанс пользователя не блокируется после определенного времени бездействия)
- ОПО.1, ОПО.2 (функционал обновления не предусмотрен в текущей версии) - Management Console

Тестирование NGFW в финансовом секторе



Не удовлетворили*

Банк России с другими банками провел тестирование российских NGFW. Со стороны вендоров в тестировании приняли участие «Код безопасности», Ideco (новогодний календарь с женщинами), PT и еще один вендор не названный. Тесты проходили на площадке ####.

NGFW показали себя хорошо на тестовых стендах, но когда начиналась серьезная нагрузка, возникало много проблем.

Банки, в частности, остались недовольны плохой стабильностью, слабой пропускной способностью и отсутствием части функционала, который был заявлен.

В ИБ-компаниях говорят, что ЦБ выбрал слишком «избыточную» методику, поэтому из 30 зарегистрированных NGFW участие в тестировании приняли только 4.

*@cybersachok

Основные принципы реализации компетентностного подхода к развитию персонала в ИБ

Начальный уровень

Единицей компетентностного подхода является компетенция, каждая из которых состоит из 5 уровней

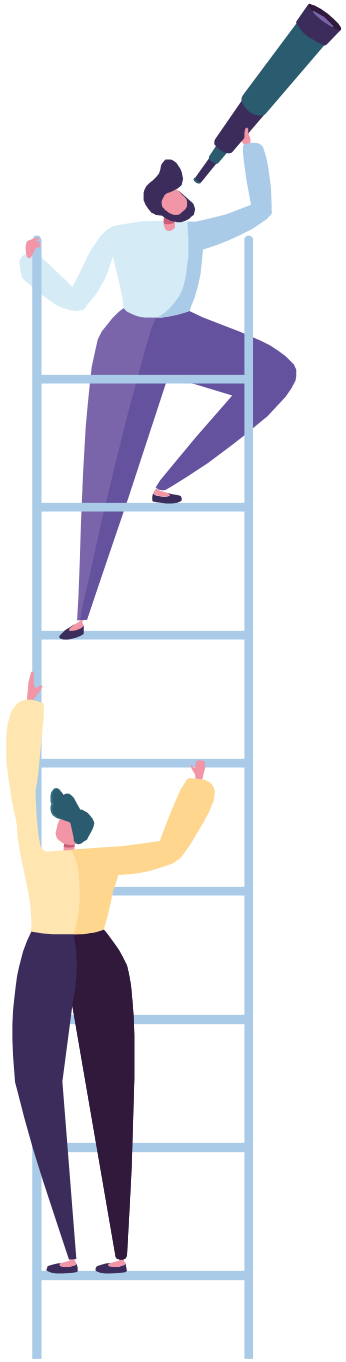
- Уровень «Базовый»: способность идентифицировать методику или технологию. Специалист имеет общее представление об областях применения методики или технологии;
- Уровень «Знание»: наличие теоретических знаний о методике или технологии. Знает порядок или процедуру их применения;

Мидл и продвинутый уровень

- Уровень «Опыт»: наличие опыта самостоятельного применения методики или технологии. Способность оценить риски применения методики или технологии в разных условиях;

- Уровень «Углубленный»: способность осуществлять технический контроль за применением методики, технологии. Способность передавать знания по предмету через консультации, наставничество или чтение курсов. Наличие опыта разработки ОРД по применению методик или технологий;

- Уровень «Эксперт»: способность самостоятельно разрабатывать или руководить разработкой новых методов или технологий. Способность провести комплексную экспертизу результатов применения.



Задачи для специалистов ИБ

Администрирование и поддержка систем защиты информации

- Мониторинг технического состояния СЗИ;
- Проведение первичной диагностики тех. состояния по результатам мониторинга;
- Осуществление первичных мероприятий по восстановлению работоспособности систем ИБ;
- Понимание назначения СЗИ, принципы работы, виды СЗИ;
- Выполнение операционной деятельности в части систем защиты информации;
- Понимание требований, предъявляемых регулятором к СЗИ

Специалист по безопасности ОКИИ

- Понимание требований законодательства, мер и процессов обеспечения ИБ объектов КИИ;
- Понимание принципов работы систем промышленной автоматизации;
- Знание способов обеспечения ИБ, применяемых в системах промышленной автоматизации
- Аудит ИБ ОКИИ (сбор исходных данных, подготовка части отчетных материалов, специфика обеспечения ИБ различных классов защищенности/категорий значимости систем ПА и ЗОКИИ);
- Категорирование ОКИИ;
- Подбор методов, способов, технологий и организационных мер, направленных на противодействие ИБ-угрозам ОКИИ, адаптация под процессы организации отраслевых/регуляторных требований по защите ОКИИ

Примеры характеристик должностей ИБ начального уровня (техник, специалист, ведущий специалист)

Профиль	Общее описание профиля	1 уровень (Базовый)	2 уровень (Знание)
Проектирование ИБ в информационных системах	Определение рисков и угроз ИБ на основе анализа информационной системы (ИС). Определение способов и средств обеспечения ИБ основных ИТ- и ИБ-вендоров. Разработка проектно-эксплуатационной документации (ПЭД). Проектирование микросервисной архитектуры и ИТ-продуктов.	Знает основные требования НПА (149-ФЗ, 152-ФЗ, 98-ФЗ, 63-ФЗ, 187-ФЗ), ГОСТов (ИСО/МЭК 27002-2021), и регуляторов (ФСТЭК, ФСБ, и др.)	Знает и умеет определять основные риски и угрозы ИБ в ИС, требования в части ИБ исходя из характеристик ИС (категории конфиденциальности, уровни доступа и т.д.) Знает составляющие элементы инфраструктуры ИС и основные риски ИБ: интеграция и трансформация данных (rabbitmq, kafka), хранение данных (redis, clickhouse, mongodb), системы виртуализации, прикладное ПО Знает средства обеспечения ИБ основных ИТ-вендоров (Microsoft, Linux, VMware и др.) и ИБ-вендоров (Kaspersky, Positive Technologies, Indeed и др.)
Проектирование ИБ в системах пром.автоматизации	Проектирование, внедрение и эксплуатация систем защиты информации систем промышленной автоматизации (далее – систем ПА) , являющихся в т.ч. ОКИИ	Знает требования по ИБ, предъявляемые регуляторами к системам ПА Имеет представление о системах ПА (назначение, состав, особенности) Имеет представление о способах обеспечения ИБ, применяемых в системах ПА (назначение, принцип работы)	Знает основные типы систем ПА Разрабатывает разделы проектной и эксплуатационной документации на системы защиты информации по поставленной задаче. Знает специфику обеспечения ИБ для систем ПА Знает основные риски ИБ систем ПА, понимает последствия для производства в случае реализации этих рисков
Системы межсетевого экранирования	Технологии межсетевого экранирования. Установка, настройка и эксплуатация межсетевых экранов. Экспертиза проектной и эксплуатационной документации в части МЭ.	Знает требования, предъявляемые регулятором к системам межсетевого экранирования Знает назначение систем межсетевого экранирования, принцип работы, виды межсетевых экранов Знает принципы модели OSI, протоколы различных уровней модели	Знает перечень и основные положения ЛНД Компании (Положение Компании «Порядок изменения политики межсетевого экрана»), регулирующие применение систем межсетевого экранирования ЕКТС Знает технологии и методы, применяемые в межсетевых экранах, основные продуктыиз данного класса систем, их преимущества и ограничения Умеет проводить пуско-наладочные работы

ЦК «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

EnergyNetCS@ya.ru