ИМБА ИТ

Импортозамещение в сфере информационной безопасности

Законодательство

1. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
2. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
3. Постановлением Правительства № 878 от 10 июля 2019 года введен Перечень радиоэлектронной продукции, происходящей из иностранных государств, в отношении которой с 1 сентября 2019 года устанавливаются ограничения для целей осуществления закупок для обеспечения государственных и муниципальных нужд
4. Постановлением Правительства РФ от 21.12.2019 №1746 установлен запрет на закупку отдельных видов товаров иностранного производства

Предпосылки

- Осложнившаяся геополитическая обстановка
- Уход с российского рынка многих вендоров
- Привязка зарубежных продуктов к зарубежной валюте, возросший ценник в рублях
- Прекращение поддержки уже закупленных продуктов в силу введенных санкций
- Участившиеся кибератаки на фоне всего изложенного выше

Вызовы

01
Необходима быстрая замена импортного ПО

02
Отсутствуют компетенции по части внедряемых вендоров

03
Отсутствует понимание, на что именно менять импортные продукты в инфраструктуре

04
Существенное влияние человеческого фактора на уровень ИБ ввиду участившихся кибератак

05
Существующий бюджет не покрывает стоимость решений для замены существующих импортных СЗИ

06
Отсутствие решений, отвечающих потребностям бизнеса

Проблемы технической поддержки

- Потеря возможности обновления ПО и прошивок устройств
- Отсутствие обновлений сигнатурных баз / баз URL
- Невозможность привлечения инженеров вендора для консультаций
- Невозможность устранить новые уязвимости в ПО и прошивках устройств
- Невозможность выявления новых образцов вредоносного ПО
- Повышенная нагрузка на собственные службы

Российские решения ИБ

Категория продукта	Заменяемый вендор	Заменяющий вендор
Защита данных		
Средства антивирусной защиты	McAfee TrendMicro Microsoft Sophos F-Secure	Bitdefender Avast Symantec Panda	kaspersky, Dr.WEB, КОД безопасности
Защита от утечек (DLP)	Symantec Forcepoint McAfee		INFOWATCH, КИБЕРПРОТЕКТ, ZECURION, ГАРДА технологии, Ростелеком, SEARCH INFORM
Защита баз данных (DAM)	Imperva IBM Oracle		ГАРДА технологии
Средства анализа защищенности, сканеры уязвимостей, управление уязвимостями (VM)	Qualys Tenable БАКОТЕК F-Secure	Rapid7 Tripwire Skybox	Эшелон, АЛТЭКС СОФТ, POSITIVE TECHNOLOGIES, Ростелеком Технологии возможностей
Контроль привилегированного доступа (PIM/PAM)	CyberArk Wallix Centrify	BeyondTrust One Identity Broadcom	АЙТИБАСТИОН, НОВЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, INDEED ID
Управление конфигурацией межсетевых экранов	Tufin Algosec	Firemon Skybox	GIS ГАЗИНФОРМ СЕРВИС
Защита почты	Fortinet FireEye Micro Focus		kaspersky, GROUP IB
Защита печати	FollowMe		SecretTechnologies
Управление доступом к неструктурированным данным (DAG/DCAP)	Varonis Imperva Netwrix	STEALTHbits	ZECURION, CYBERPEAK, ОРЛАН, SEARCH INFORM, ГАРДА технологии
Сбор, обработка и хранение событий по ИБ (SIEM)	IBM Security Micro Focus Microsoft	Fortinet McAfee	Эшелон, kaspersky, POSITIVE TECHNOLOGIES, GIS ГАЗИНФОРМ СЕРВИС, SEARCH INFORM, Rusiem
Противодействие мошенничеству (Fraud Prevention)	Intellinx		kaspersky, GROUP IB, ГАРДА технологии, FUZZY LOGIC LABS
Анализаторы кода	Checkmarx Micro Focus		POSITIVE TECHNOLOGIES, Ростелеком Технологии возможностей, INFOWATCH

Категория продукта	Заменяемый вендор	Заменяющий вендор
Сетевая безопасность		
Межсетевые экраны **(Firewalls)**	Check Point Palo Alto Fortinet Cisco Juniper	КОД безопасности, UserGate, ideco
Защита веб-приложений (WAF)	Imperva F5 A10 Radware	КОД безопасности, Positive Technologies
Контроль доступа в сеть NAC	Cisco ISE ForeScout Fortinet Portnox	NETAMS
Защита от целевых атак (песочницы)	Check Point Palo Alto Fortinet Trend Micro Microsoft FireEye Forcepoint McAfee	kaspersky, AVSOFT, Positive Technologies
Системы выявления аномалий, анализа трафика, визуализации сети (NTA)	Cisco Fiowmone Arbor	kaspersky, GROUP IB, Positive Technologies, МФИ СОФТ
Защита каналов связи (VPN)	Check Point Palo Alto Fortinet Cisco Juniper	КОД безопасности, infotecs, s•terra, Специальная интеграция
Сервисы защиты от DDos-атак	Arbor Radware	kaspersky, radware, QRATOR LABS, ГАРДА технологии, servicepipe, BIFIT

Использование open-source решений

Категория продукта	Продукт
Сетевая безопасность	
Межсетевые экраны (Firewalls)	pfsense
Система обнаружения вторжений (IDS)	SURICATA, SNORT
Защита веб-приложений (WAF)	Nemesida WAF
Оценка уязвимостей (VA)	WAZUH, OpenVAS, NMAP.ORG
Контроль доступа в сеть (NAC)	PacketFence
Antispam	ANTI-SPAM SMTP PROXY SERVER
Защита от целевых атак (песочницы)	CUCKOO
Защита данных	
Средства антивирусной защиты (Antivirus)	ClamAV
Хостовая система обнаружения вторжений (HIDS)	OSSEC, WAZUH
Тестирование безопасности (Security Testing)	
Контроль привилегированного доступа (PAM)	JUMPSERVER
Система управления идентификацией и доступом (IAM)	OpenIAM
Оценка безопасности (Security Assesment)	Gophish
Двухфакторная аутентификация (2FA)	LinOTP
Сбор, обработка и хранение событий по ИБ (SIEM)	OSSEC, WAZUH, ALIEN VAULT OSSIM, elastic
Платформа реагирования на инциденты на IRP	TheHive

Чем может помочь ИМБА ИТ

Разработка дорожной карты импортозамещения

Позволяет получить четкое понимание, какие именно решения нужно менять, каков бюджет, сроки и приоритеты

Экспресс анализ защищенности внешней инфраструктуры

Определит "слабые" места в инфраструктуре компании, позволит понять критичность угроз и приоритет их устранения

Демонстрация решений ИБ в нашей лаборатории

Позволяет ознакомиться и получить представления о основных возможностях решений ИБ

Пилотирование решений ИБ в вашей ИТ-инфраструктуре

Позволяет апробировать решения в вашей ИТ-инфраструктуре, оценить возможности и работоспособность решений в вашем ИТ-ландшафте

Подбор и сайзинг ИБ решений вместо зарубежных

С учетом нашего опыты мы поможем вам подобрать оптимальное решение под ваши задачи и бюджет

Внедрение поставляемых решений

Позволит избежать ошибок при внедрении, ускорит ввод в промышленную эксплуатацию

Поддержка после внедрения

Упростит процесс освоения решений Вашими специалистами, ускорит решение проблем

Обучение для Ваших сотрудников

Даст необходимую теоретическую основу, ускорит освоение новых решений

Наша лаборатория

Вы можете ознакомиться с любым из решений ИБ в нашей лаборатории в режиме онлайн-кабинета.

Вендор	Группа	Продукт	Пилот	Демостенд	*Техническая поддержка
positive technologies	SIEM	MaxPatrol SIEM	✓	✓	✓
kaspersky	SIEM	KUMA	✓	✓	✓
INFOWATCH	DLP	Traffic Monitor	✓	✓	✓
positive technologies	WAF	PT AF	✓	✓	✓
КОД безопасности	Firewall	АПКШ Континент	✓	✓	✓
UserGate	Firewall	UserGate	✓	✓	✓
kaspersky	Antivirus	Kaspersky Security для бизнеса	✓	✓	✓
АЙТИБАСТИОН	PAM	СКДПУ	✓	✓	✓
Новые технологии безопасности	PAM	Safeinpect	✓	✓	✓
kaspersky	Mail Security	Kaspersky Security для почтовых сервисов	✓	✓	✓
КОД безопасности	VPN	АПКШ Континент	✓	✓	✓
s•terra	VPN	С-Терра Шлюз	✓	✓	✓
positive technologies	VA	MaxPatrol VM	✓	✓	✓
NETAMS	NAC	WNAM	✓	✓	✓
positive technologies	NTA	PT NAD	✓	✓	✓
LinOTP	2FA	LinOTP	✓	✓	✓
WAZUH	SIEM	Wazuh	✓	✓	✓

*по согласованию, на коммерческой основе

ping@imba-it.ru
imbasec.ru