Что значит КИИ для оператора связи: 2025 не за горами

Вступление

Кажется, провайдеры и операторы связи стали забывать про требования законодательства.

Впервые про термин КИИ в России услышали с выходом Федерального закона № 187 ФЗ, который создал правовую базу для присвоения информационным системам, информационно-телекоммуникационным системам, автоматизированным системам управления - «критического» статуса.

Это значило лишь то, что любая компания, работающая в стратегических сферах экономики, будь это наука, здравоохранение, транспорт, энергетика, банковская сфера, связь, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, которые налаживают и обеспечивают взаимодействие информационных систем или сетей для перечисленных структур – становятся **субъектами критической информационной инфраструктуры**.

На различных производствах построены сети, в которых есть автоматизированные системы управления (или же, АСУ) – такие информационные системы, в рамках закона, и называются **объектами критической информационной инфраструктуры,** которая непременно должна защищаться различными средствами защиты информации, иначе, в случае **компьютерного инцидента**, который, впоследствии выведет такие системы из строя, могут быть человеческие жертвы и серьезный урон экологии.



Проблематика

Итак, мы с вами разобрались, что такое КИИ и кого мы можем называть субъектом критической информационной инфраструктурой. Но что насчет ответственности и требований по информационной безопасности?

В начале я оставил слова про провайдеров, потому что в информационном мире бывают своеобразные поставщики услуг, и по схеме взаимодействия объектов КИИ они становятся посредником, который тоже становится КИИ, но с условием. Звучит это, немного странно, но по правилам, предусмотренным законом **N 187- ФЗ**, отнесение любого ИП, российского юридического

лица, государственного учреждения и государственного органа к субъектам КИИ осуществляется по:

- Виду деятельности или сфере деятельности (8 пункт, статьи 2).
- ОКВЭД относится к одному из перечисленных выше секторов экономики.
- **Праву собственности, аренды или на ином законном основании любые ИС, ИТКС и АСУ.**
- Факту обеспечения взаимодействия **ИС, ИТКС** и **АСУ**, принадлежащих государственному органу, государственному учреждению, российскому юридическому лицу и/или ИП, осуществляющих свою деятельность в одной или нескольких сферах деятельности, предусмотренных пунктом 8, статьи 2.

Имея в наличии даже один из этих критериев субъекта КИИ, предоставляя услуги по виду деятельности или сфере деятельности, указанных в **ФЗ 187**, провайдер сразу становится субъектом КИИ, а его инфраструктура – объектом КИИ.

ВОЗМОЖНЫЕ УГРОЗЫ	ОБЪЕКТЫ ВОЗДЕЙСТВИЯ													ХАРАКТЕРИСТИКА УГРОЗЫ
	Оборудование ИС, ИТКС, АСУ	Пользователи ИС, ИТКС, АСУ	Обеспечивающий персонал	Центр обработки данных	Серверное оборудование	Телекоммуникационное оборудование	Исполнительные устройства	Сетевое оборудование	Технологическое оборудование	Программные компоненты для передачи данных по сетям	Файлы данных (информация)	Базы данных с информацией	Прикладные программы доступа и обработки информации	
Угрозы создания нештатных режимов работы	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	ДА	ДА	НЕТ	НЕТ	ДА	Преднамеренные изменения служебных данных, игнорирование предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажение (модификация) самих данных
Угрозы доступа (проникновения) в операционную среду	ДА	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	НЕТ	НЕТ	ДА	Несанкционированный доступ к информации или внедрение вредоносных программ путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия
Угрозы удаленного доступа (сетевые атаки)	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	ДА	ДА	НЕТ	ДА	ДА	ДА	ДА	Захват контроля (повышение прав) над удалённой ИС, ИТКС, АСУ, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, осуществляемое по каналам связи
Угрозы	НЕТ	НЕТ	НЕТ	ДА	ДА	ДА	НЕТ	ДА	НЕТ	ДА	ДА	ДА	ДА	Воздействие на ИС, ИТКС, АСУ с помощью

Существуют категории КИИ, которые делятся, непосредственно, на три категории:

- (III) Третья – младшая категория.
- (II) Вторая – средняя категория.
- (I) Первая – самая высокая.

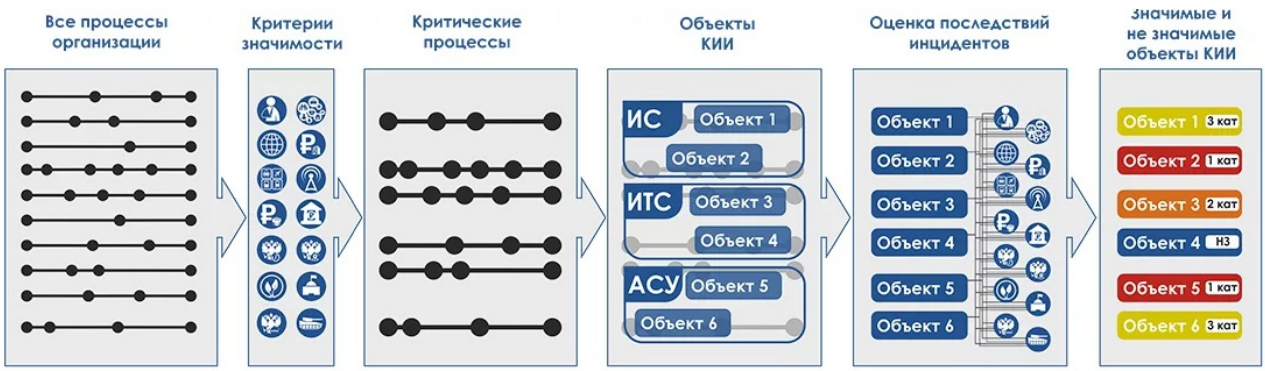
Несмотря на наличие каких-либо объектов КИИ, эти объекты не всегда бывают **значимыми**. Для любого оператора связи «критическим» приговором может стать предоставление своих услуг определенному числу абонентов – от 3000 человек. От этого числа провайдер получает свою категорию значимости – **третью**, согласно таблице с критериями в **ПП РФ №127**

Даже если провайдер не имеет **значимых** объектов критической информационной инфраструктуры, он обязан провести инвентаризацию следующих систем:

- Информационных.
- Программных.
- Технических.

Параллельно, необходимо выявить те самые критические события: сбои, остановка работы каналов связи, которые приведут к негативным социальным, политическим и экономическим последствиям.

Операторам связи, оказывающим услуги для государственных органов власти, необходимо рассмотреть негативные последствия в виде возникновения ущерба бюджетам РФ (федерального, субъекта РФ, внебюджетных фондов) и нарушение или прекращение функционирования органа власти в возложенного на его функции.



А что с информационной безопасностью?

Операторы связи живут в своей сфере, принимая трафик по брасам, иногда перебирают агрегацию сети.

Информационная безопасность тоже требует внимания. В любой организации должны быть свои SOC (Security Operation Center), хотя бы один человек, который будет согласно политикам и/или регламентам следить за порядком в сети и искать отклонения в миллионе логов, аккуратно сосредоточенных в предназначенных для этого системах.

В информационно-правильной системе должен быть «бумажный» специалист по безопасности, который следит за всеми регламентами, следит и отвечает за порядком их исполнения. Как правило, этот ИБ-шник не сидит перед экраном в интерфейсе EDR, SIEM, NTA-системами и не знает как с ними работать. Его задача – грамотно написать «программу» по планированию, проектированию, подбору, внедрению и сопровождению перечисленных ранее систем.

И есть тот самый офицер информационной безопасности, который знает как работает вся инфраструктура и через сколько фильтров проходит трафик, прежде чем выйти в глобальную сеть и наоборот. В каких-то организациях этот человек один – он занимается мониторингом и устранением уязвимости или инцидентами безопасности. Но, по феншую офицер безопасности как система SOAR – он тот самый начальник, который дает рядовым инженерам по обязанности, и, так он налаживает процессы в одной глобальной задаче – обеспечивать информационную безопасность в компании.

Но что, если на данный момент оператор связи имеет свою привычную инфраструктуру из коммутаторов и маршрутизаторов, которые обеспечивают работу всего бизнеса, и, казалось бы, всё просто замечательно, а тут распределенная атака на отказ оборудования, брут внутренних административных ресурсов с клиентских ПК, сайт повис насмерть... ? Для компании перечисленные события как нечто противное и неприятное, когда кто-то другой копается в сети или пытается её уронить, но, в случае, если сеть оператора связи упадет – это потеря доходов и множество недовольных клиентов, которые в любой момент могут разорвать договор и уйти к конкуренту.

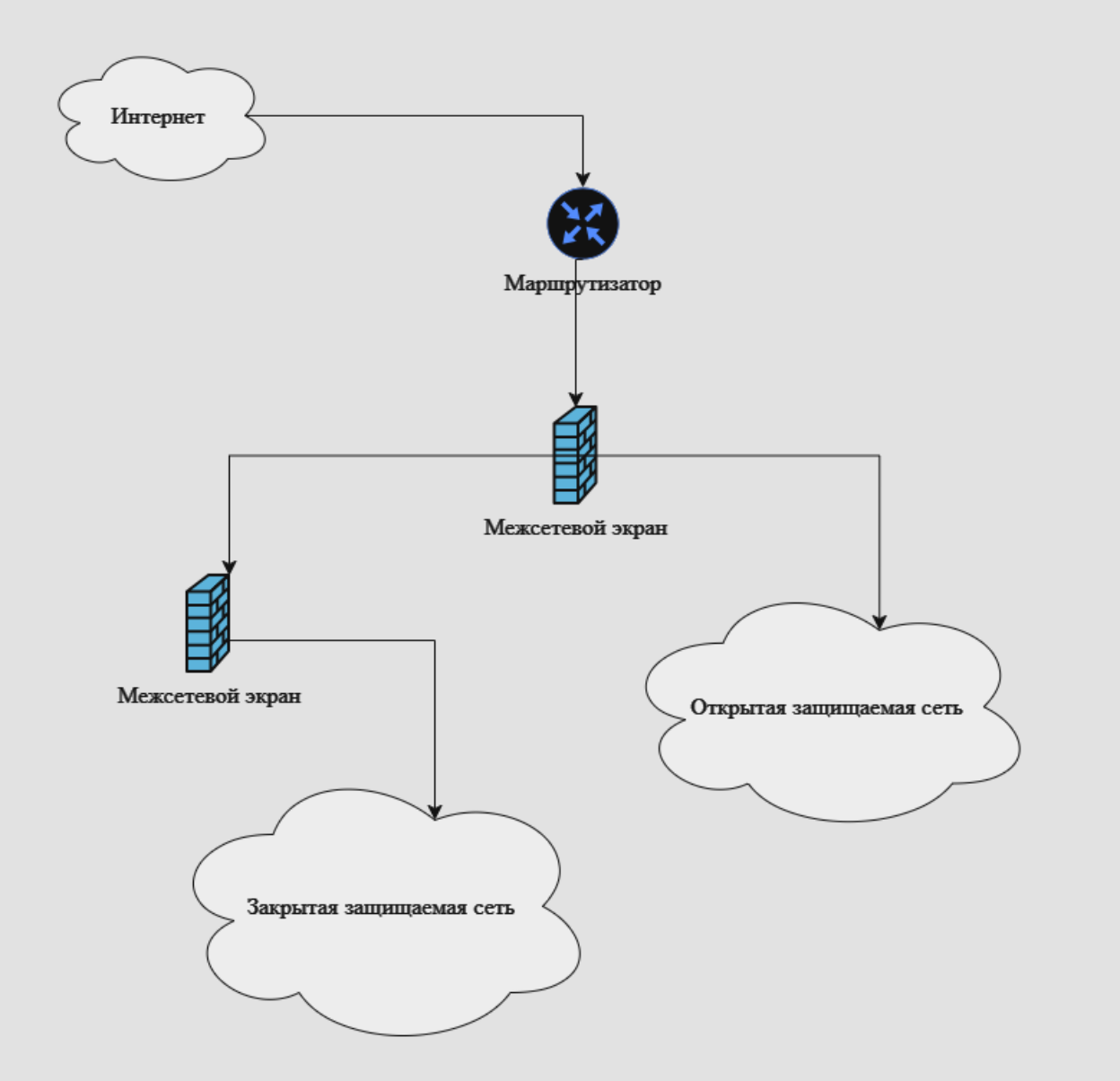
С чего начать?

Скажем так, любой провайдер старается соблюдать законодательство, чтобы его не душили штрафами, взысканиями и проверками, а это – РКН, СОРМ, Яровая.

Теперь, каждый провайдер должен защищаться, и не просто от взысканий, а от угрозы безопасности, которая может реализоваться в любой момент. Это больше не "русская рулетка" с "пулями", а требование законодательства, потому что многие провайдеры являются связующими точками в большой информационной инфраструктуре Российской Федерации.

После проведенных мероприятий инвентаризации сети, уведомления в органы власти, разработки плана **X** – нужно действовать. Миллионы ACL на коммутаторах могут сделать супер-правильный строй трафика и защитить от «дурака», но не защитит от реальных атак. Поэтому, для начала, необходимо задуматься об шлюзе безопасности. Сейчас это называется NGFW - Next Generation FireWall, потому что это целый кухонный комбайн в сфере информационной безопасности, в нем есть защита от DDoS, правила межсетевого экрана, система обнаружений вторжений, потоковый антивирус, VPN, SSL-инспекция трафика, фильтрация контента и прочее.

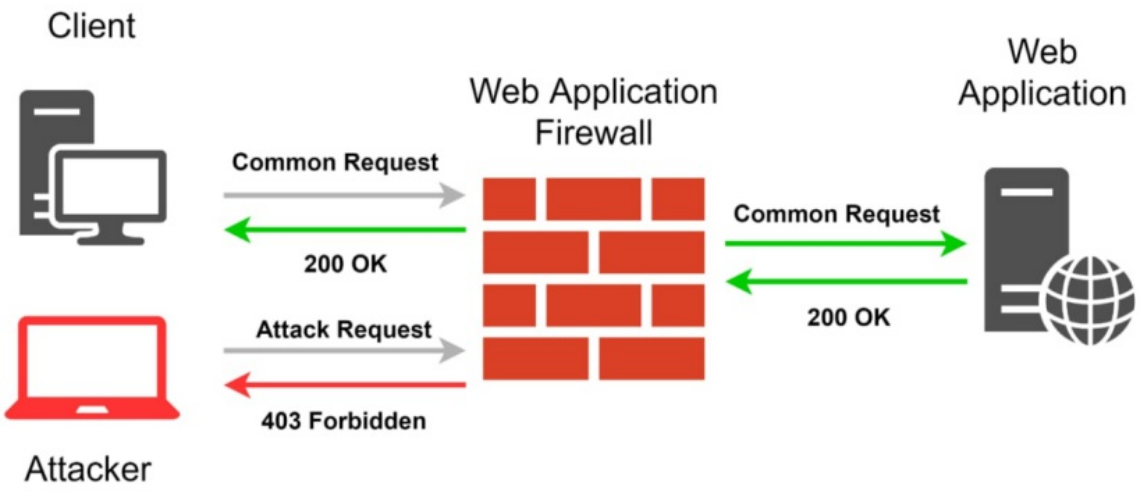
Межсетевой экран должен стать стеной между глобальной сетью и корпоративными сегментами, чтобы весь сетевой трафик инспектировался и из него исключались несанкционированные действия на базе сигнатур известных атак, а также, чтобы обнаружить нарушения политики безопасности и фильтровать спам как снаружи, так и внутри.



Это очень важно для любой компании, межсетевые экраны должны стоять в любой инфраструктуре, а для провайдеров это особенная тема: когда каждый день кого-то атакуют, и эти атаки не заканчиваются одними DDoS’ами.

У каждой организации есть своё веб-лицо – сайт, на котором есть информация об деятельности компании, возможно есть авторизация и даже платежные механизмы. Всё это тоже требует наблюдения и постоянной защиты от злоумышленников, потому что, банально, есть атака до отказа на L7-уровне, который положит сайт и может серьезно нагрузить сервер.

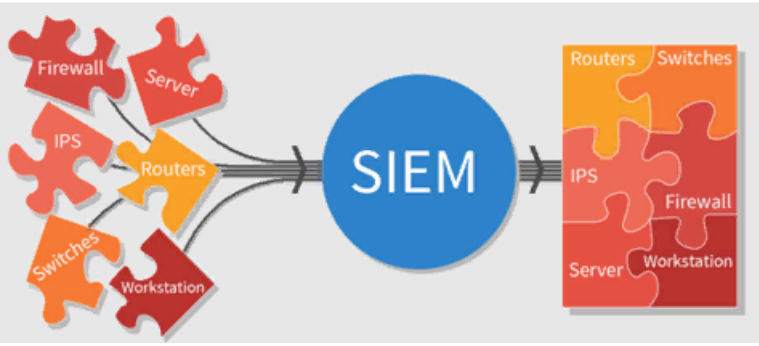
Это решение класса Web Application Firewall – такой межсетевой экран работает на прикладном уровне и предназначен для защиты от атак HTTP-запросами к серверу, которые могут скрывать в себе серьезную угрозу, впоследствии открывающую дыру в защите инфраструктуры компании. Можно потратить время и привести в порядок все конфигурации сервера и сайта, защитив от 10-15% атак, но этого недостаточно - в подавляющем большинстве веб-ресурсов есть уязвимости, и, при необходимости, злоумышленник будет перебирать все способы. В конце концов, сервер сам себя не защитит от атак на логику ресурса, перебивания буфера бесконечным количеством HTTP-запросов.



Внутри инфраструктуры можно и нужно устранять лишний доступ, составлять политики доступа для группы лиц и не допускать неавторизованный доступ до каких-либо ресурсов или сегментов сети. От подобных угроз защищают различные NAC-продукты, завязанные на технологии Endpoint Security – это не защита эндпоинтов от конкретных атак, это защита «друг от друга». Кто-то пользовался Cisco ISE, но в текущих реалиях, пришло время импортозамещаться.

Также, помимо NAC, есть узконаправленные решения типа Access Manager, которые не дают пользователю доступ до корпоративной сети и выход в глобальную сеть, пока не будет выполнена двухэтапная аутентификация, и пользователь не будет авторизован.

Когда в сети уже очень много оборудования, отовсюду плывет много трафика, и при этом, необходимо отслеживать подозрительные активности – требуется концентрация логов в SIEM (Security Information and Event Management). Решение этого типа собирает в себя события из различных источников, которые можно интегрировать, например – IDS, DLP, APM, маршрутизаторы.



Все события с устройств создают накопленную статистику. Тем самым, SIEM может сгенерировать событие безопасности, если произошло что-то, выходящее за рамки привычных сценариев. Например, сотрудником с соответствующими правами отправляется чувствительная информация по адресу, который не должен получать эту информацию. Также, производители поставляют свою экспертизу с различными вариантами инцидентов.

Говоря об инцидентах, бывают совсем неочевидные события, которые вручную расследовать крайне сложно и долго. Для обнаружения факта события безопасности в ретроспективе, либо происходящего вторжения, придумано решения класса NTA (Network Traffic Analysis). NTA помогает найти в копии L2-L7 трафика следы атаки, работая с зашифрованным трафиком. Также, находит признаки нарушения регламентов ИБ (нелегальные протоколы, отправка информации в открытом виде), выявляет модифицированные ВПО.

Все перечисленные решения являются базой в современной парадигме информационной безопасности. Настоятельно рекомендую подумать, где в сети не хватает межсетевого экрана и переосмыслить отношение к безопасности собственной инфраструктуры.

Итоги

Операторы связи должны обратить внимание на важность проблемы. Информационная безопасность – это безопасность вас самих. В любой организации должен быть офицер ИБ, который поддерживает

соблюдение регламентов и тот, кто поддерживает работу СЗИ в инфраструктуре. Первым шагом в обеспечении безопасности является наведение порядка в информационном взаимодействии во внутренней и внешней сети и установка базовых средств защиты информации.

От этого не сбежишь, когда условия диктует государство.