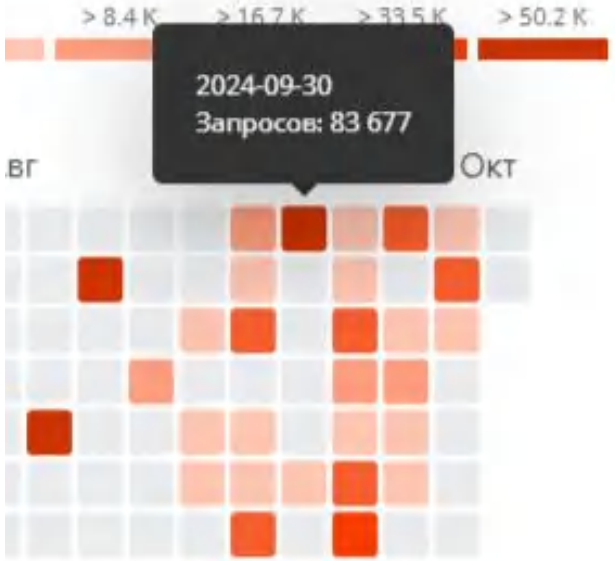
Анализ событий безопасности

Буторин Денис Владимирович,
Инженер по защите информации,
Отдел информационной безопасности
Центра цифровой трансформации образования
Кировской области,
КОГОАУ ДПО «ИРО Кировской области»

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

Защита от DDoS-атак

DDoS-атака (Distributed Denial of Service) — это форма кибератаки на веб-системы с целью вывести их из строя или затруднить доступ к ним для обычных пользователей

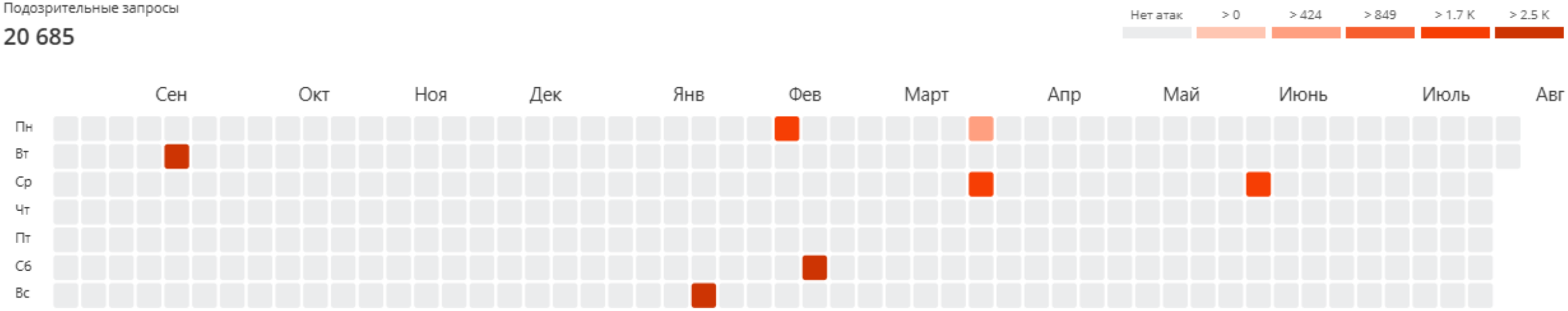


ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

Защита от DDoS-атак

Статистика атак

Подозрительные запросы
20 685

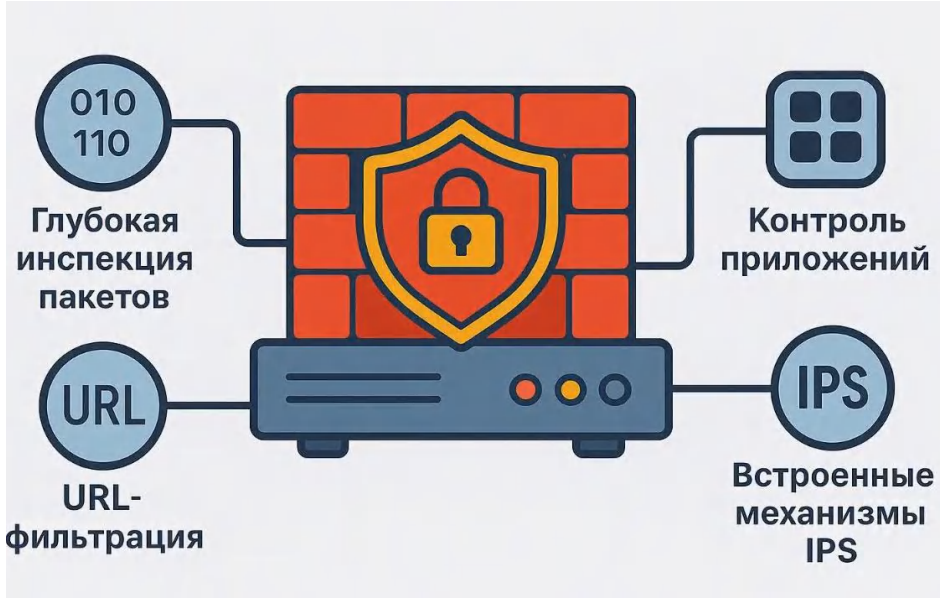


NGFW

NGFW (Next-Generation Firewall) — это **межсетевой экран нового поколения**. Это продвинутая система сетевой безопасности, которая не просто фильтрует трафик по портам и IP-адресам, но и глубоко анализирует его содержимое, чтобы выявлять сложные современные угрозы.

Ключевые функции NGFW:

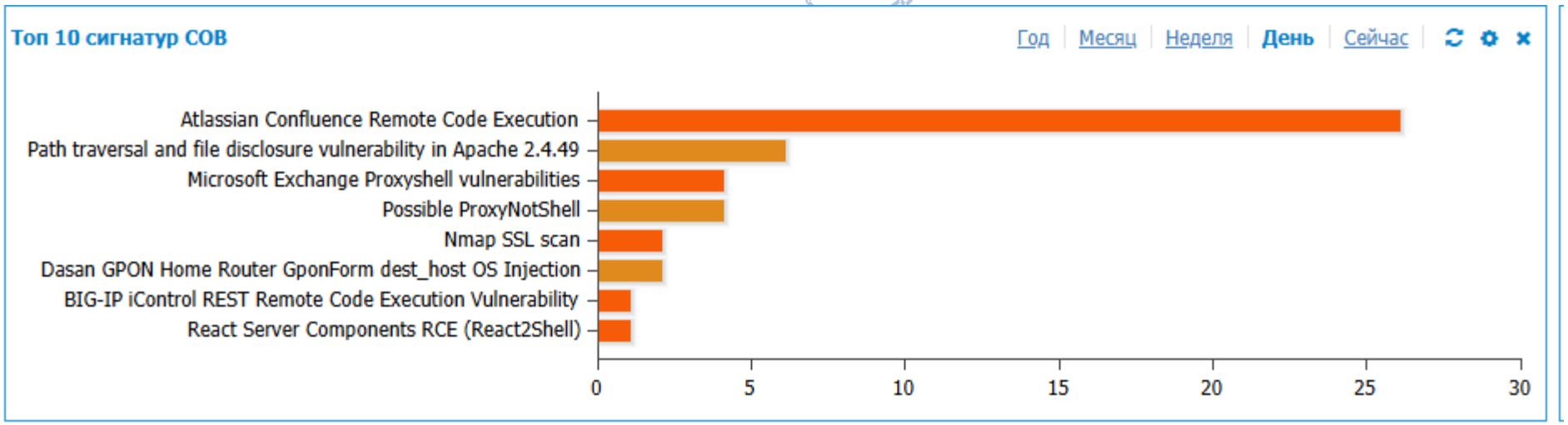
1) Контроль приложений (Application Control)
2) Глубокое инспектирование пакетов (DPI — Deep Packet Inspection)
3) Система предотвращения вторжений (IPS)
4) Идентификация пользователей (User Identity)
5) Инспектирование зашифрованного трафика (SSL/TLS Decryption)
6)Антивирусная защита и песочницы (Sandboxing)



Топ 10 доменов по количеству запросов

Атаки перехваченные на NGFW

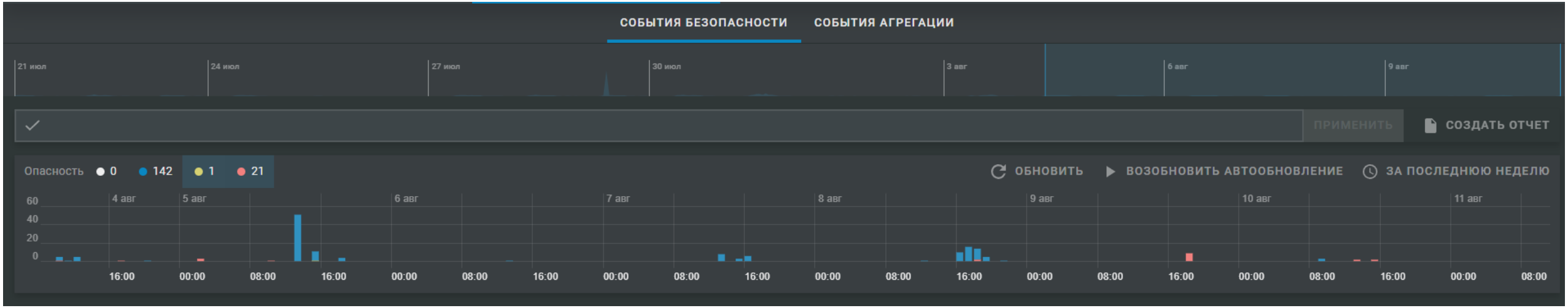
ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ



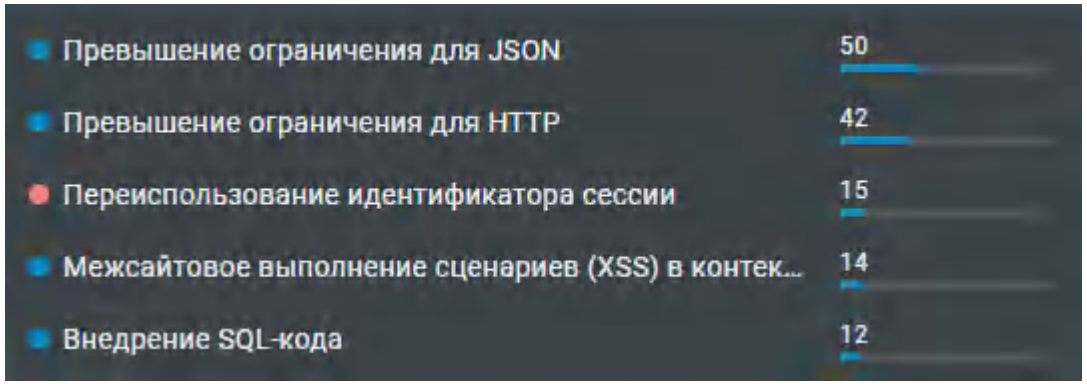
ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

WAF

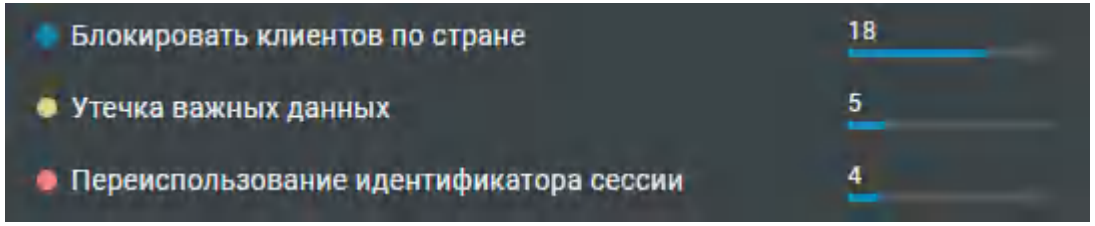
WAF (Web Application Firewall) — это **межсетевой экран уровня веб-приложений**. В отличие от NGFW, который защищает всю сеть целиком, WAF создан специально для защиты **конкретных веб-сайтов, веб-сервисов и API** от атак, направленных на уязвимости в самом коде приложения.



WAF


Превышение ограничения для JSON 50
Превышение ограничения для HTTP 42
Переиспользование идентификатора сессии 15
Межсайтовое выполнение сценариев (XSS) в контек... 14
Внедрение SQL-кода 12

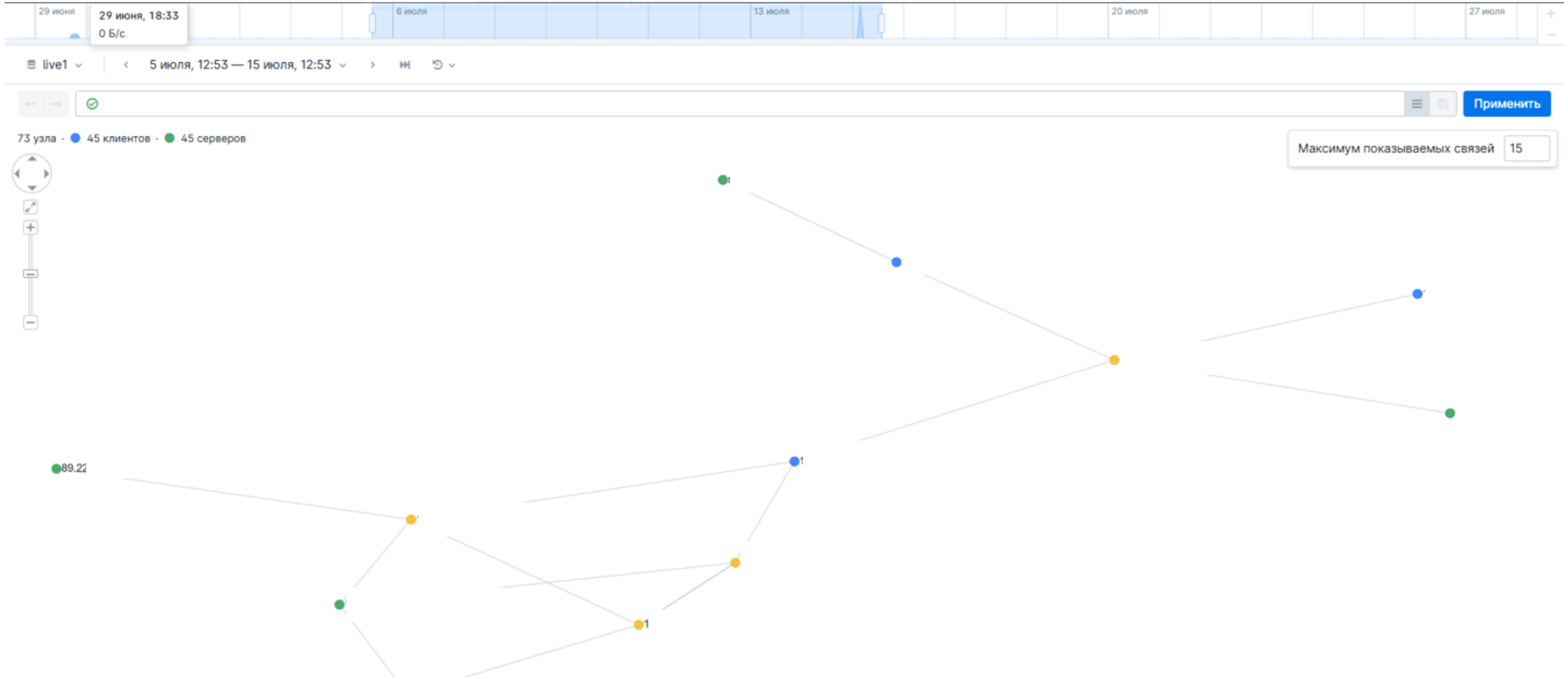

User-Agent бота 4
Внедрение SQL-кода 1


Блокировать клиентов по стране 18
Утечка важных данных 5
Переиспользование идентификатора сессии 4

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

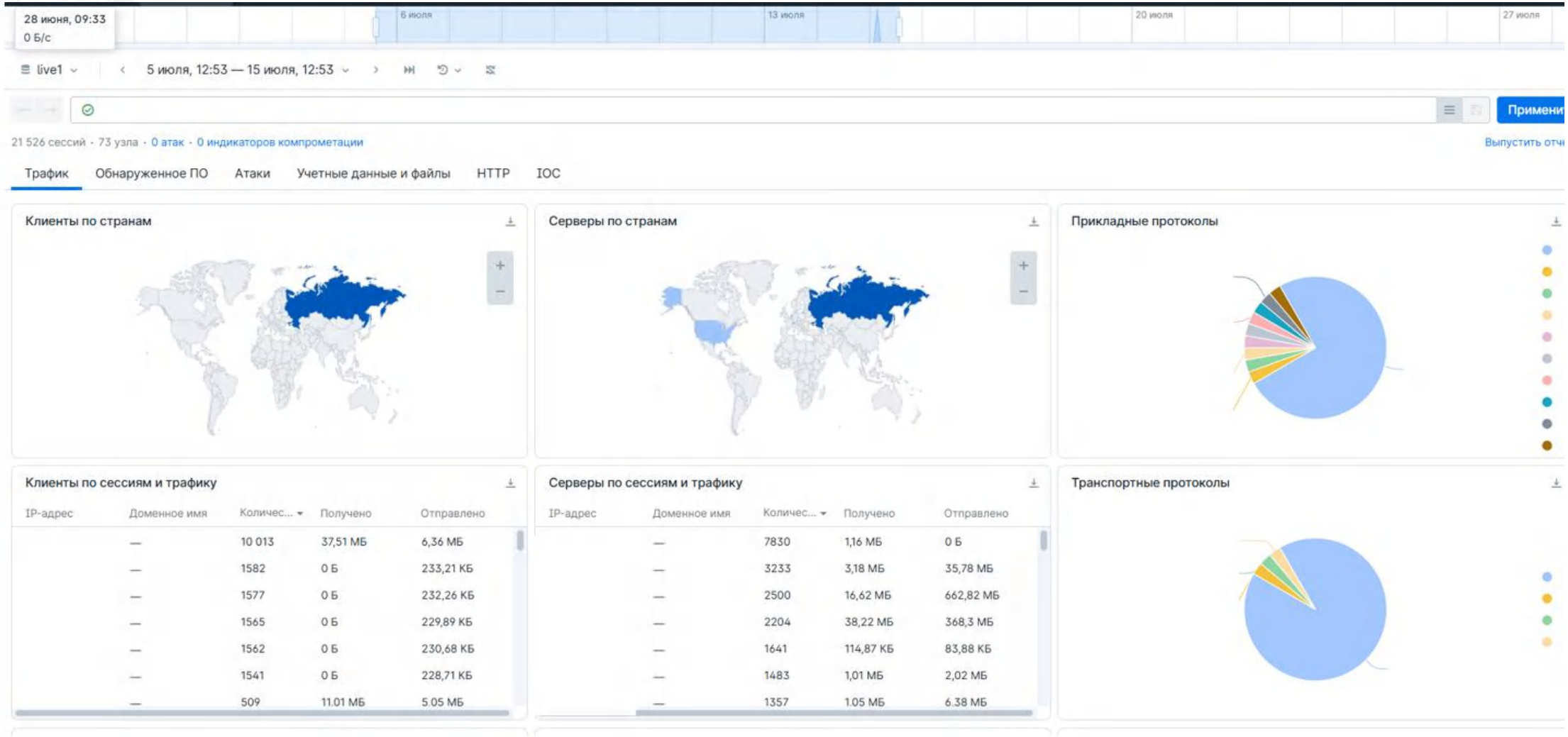
NTA

NTA (Network Traffic Analysis) — это класс решений информационной безопасности, которые выявляют угрозы, атаки и аномалии, анализируя копию сетевого трафика.



ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

NTA



ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

NTA

Узлы | Изменить тип и роли | Изменить название | Сбросить изменения

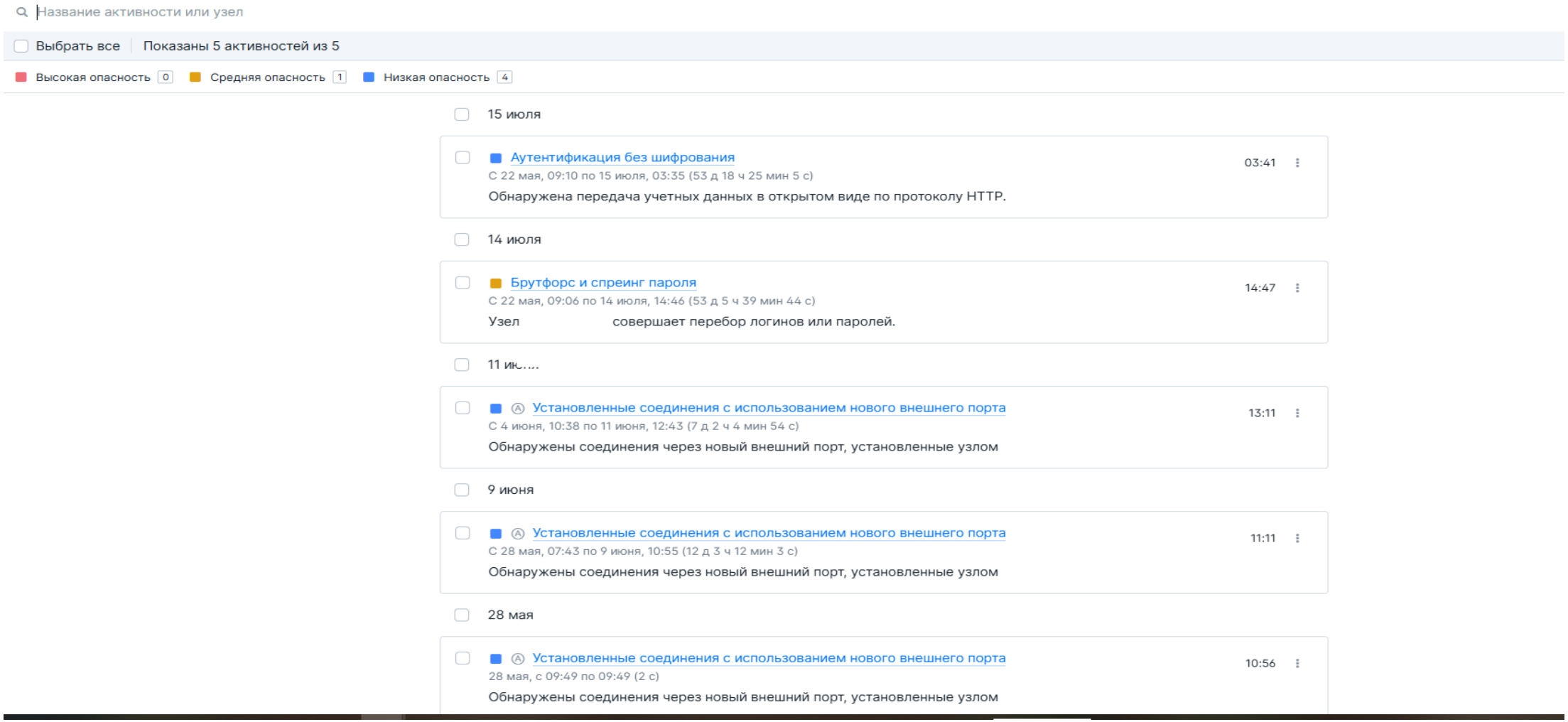
Узел | Тип | Роль | Группа | Вход. трафик (протокол, баннер, порт | Исход. трафик (протокол, баннер) | Ещ

24 узла, выбран 1 узел · 4 рабочие станции · 11 серверов · 0 сетевых устройств · 0 мобильных устройств · 0 принтеров · 9 неизвестны

Идентификатор	Название	IP-адрес	Роли	Группы	Домены	ОС	Входящий трафик	Исходящий трафик	Логины во вход. трафике	Логины в исх. трафике
H9	Не задано		Сервер базы дан...	HOME_NET						
H10	Не задано			HOME_NET						
H23	Не задано			HOME_NET						
H24	Не задано			HOME_NET						
H7	Не задано			HOME_NET						
H1	Не задано			HOME_NET						
H6	Не задано			HOME_NET						
H17	Не задано		Файловая служба	HOME_NET		Linux	nfs	ntp		
H8	Не задано		Сервер базы дан...	HOME_NET		Linux	postgresql, mongo...	nfs, zabbix, ntp		
H2	Не задано			HOME_NET						
H5	Не задано			HOME_NET						
H25	Не задано			HOME_NET						
H4	Не задано			HOME_NET						
H11	Не задано			HOME_NET						
H12	Не задано			HOME_NET						
H14	Не задано			HOME_NET						
H22	Не задано			HOME_NET						
H21	Не задано			HOME_NET						
H20	Не задано			HOME_NET						

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

NTA



ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
КИРОВСКОЙ ОБЛАСТИ

Контакты

КОГОАУ ДПО «Институт развития образования Кировской области»
Отдел информационной безопасности ЦЦТО КО
Буторин Денис Владимирович
Инженер по защите информации
Электронный адрес: dv.butorin@kirovipk.ru
г. Киров, ул. Р. Ердякова, д.23/2. тел. 8(8332) 255-442, доб. 272