

From: ["Кузнецов Александр Васильевич" <MAILER-DAEMON>](#)
To: ["Шобонов Александр Германович"](#)
Date: 10/4/2022 5:13:30 AM
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Саша, проговорил с Мананским, понятнее не стало. Он сказал, что сам не против поговорить с представителями Касперского на этот счет, от чего я само собой отказался.

С технической точки зрения у них не должно быть сложностей с ограничением доступа к URL-адресам с протоколом https, поскольку шифрование, про которое говорят представители Касперского в своих ответах, происходит на этапе соединения клиента с сервером. Их задачей является ограничение доступа к ресурсам при запросе в адресной строке ресурса URL с протоколом https, как они делают уже например с ip-адресами, к которым изначально при обычном вводе ip-адреса в адресной строке браузера получить доступ не получится (они реализовали ограничение доступа к ip-адресам «Заглушкой Касперского», в чем сложность сделать точно также с https не ясно). При чем при запросе ip-адреса в адресной строке – соединения клиента с сервером в целом не происходит, это работает только если клиент и сервер находятся в одной внутренней сети.

Суважением,
Кузнецов Александр
Тел. +7 (925) 261-82-10

From: Кузнецов Александр Васильевич
Sent: Monday, October 3, 2022 3:57 PM
To: Шобонов Александр Германович
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Саша, предлагаю следующий проект письма ЕЮ, но хочу сперва поговорить с Мананским для уточнения возможности блокировки HTTPs - соединений:

«Евгений Юрьевич, добрый день!

В ответ на письмо от 30.09.2022 получен ответ от представителей Касперского. От работы с файлом, направленным 30.09.2022 представитель Касперского отказался поскольку они получают XML-файл выгрузки.

Представитель Касперского задал вопрос, возможно ли добавить тип блокировки по домену для URL-адресов с протоколом https в XML-выгрузку. При смене типа блокировки для URL-адресов с протоколом https в файле XML выгрузки Касперский сможет заявить, что получает от Роскомнадзора некорректную выгрузку, поэтому **предлагается** направить ответ «Добавить в файл XML выгрузки **blocktype = "domain"** к URL-адресам с протоколом HTTPs не представляется возможным.». Помимо этого **предлагается** уточнить мобильный телефон представителя Касперского - Ласточника Павла и посредством мобильной связи связаться для уточнения проблемы связанной с ограничением доступа к URL-адресам с протоколом HTTPs.

Предлагается направить следующий ответ представителям Касперского:

«Добрый день!

Добавить в файл XML выгрузки **blocktype = "domain"** к URL-адресам с протоколом HTTPs не представляется возможным.

Павел, просим сообщить мобильный телефон для связи.

Предлагаем проговорить голосом проблему с ограничением доступа к URL-адресам с протоколом HTTPs.»»

Суважением,
Кузнецов Александр
Тел. +7 (925) 261-82-10

From: Кузнецов Александр Васильевич
Sent: Monday, October 3, 2022 2:36 PM
To: Шобонов Александр Германович
Сс: Теплоухов Аркадий Константинович
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

По прежнему не до конца понятно в чем проблема на стороне Касперского разрывать соединения для URL-адресов с
2/8/2023

протоколом HTTPs. Хотелось бы проговорить с представителем Касперского «Голосом» эту проблему, поскольку изменять тип блокировки для URL-адресов с протоколом HTTPs в выгрузке мы не можем, список ресурсов в виде csv - файла для них не подходит, отбирать популярные ресурсы в выгрузке и указывать для Касперского только то, что не популярно мы тоже не можем (получится так, что мы что-то блокируем, а что-то нет, почему? Потому что). Однако все это не отменяет того, что они обязаны по закону фильтровать все ресурсы, которые находятся в ФГИС. Нужно подумать, рациональных предложений на текущий момент у меня нет.

*С уважением,
Кузнецов Александр
Тел. +7 (925) 261-82-10*

From: Шобонов Александр Германович
Sent: Monday, October 3, 2022 2:08 PM
To: Кузнецов Александр Васильевич
Сс: Теплоухов Аркадий Константинович
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Если мы отклоняем их просьбу, получается, решения нет?

From: Кузнецов Александр Васильевич
Sent: Monday, October 03, 2022 1:55 PM
To: Шобонов Александр Германович <a.shobonov@int.grfc.ru>
Сс: Теплоухов Аркадий Константинович <A.Teplouhov@rkn.gov.ru>
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Чтобы не затрагивать весь домен нужно блокировать URL-адрес с указанным протоколом (http, https). По-другому не затрагивать весь домен не получится.

*С уважением,
Кузнецов Александр
Тел. +7 (925) 261-82-10*

From: Шобонов Александр Германович
Sent: Monday, October 3, 2022 1:54 PM
To: Кузнецов Александр Васильевич
Сс: Теплоухов Аркадий Константинович
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

А как вообще блокировать такие адреса, не затронув весь домен?

From: Кузнецов Александр Васильевич
Sent: Monday, October 03, 2022 1:53 PM
To: Шобонов Александр Германович <a.shobonov@int.grfc.ru>
Сс: Теплоухов Аркадий Константинович <A.Teplouhov@rkn.gov.ru>
Subject: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Помимо этого непонятно тогда каким образом они собираются блокировать запрещенные URL-адреса например youtube, исходя из их письма блокировать они их не будут в принципе.

*С уважением,
Кузнецов Александр
Тел. +7 (925) 261-82-10*

From: 276-fz [<mailto:276-fz@rkn.gov.ru>]
Sent: Monday, October 3, 2022 1:46 PM
To: Шобонов Александр Германович
Сс: Теплоухов Аркадий Константинович; Кузнецов Александр Васильевич
Subject: FW: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Саша, поступил ответ представителей Касперского.

В письме сообщается, что осуществлять ограничение доступа к URL-адресам с протоколом https они не могут исходя из файла с доменными именами URL-адресов с протоколом https.

Если мы добавим к URL-адресам с протоколами https в выгрузку тип блокировки по домену (**blocktype = "domain"**), то они смогут заявить, что они получают от Роскомнадзора некорректную выгрузку. Поэтому и создавался отдельный файл в доменах URL-адресов с протоколами https.

Чистить файл выгрузки от популярных ресурсов, о которых представить Касперского упоминает в письме, очень трудозатратное занятие.

Исходя из вышеуказанного, предлагаю ответным письмом направить: «Добавить в файл XML выгрузки **blocktype = "domain"** к URL-адресам с протоколом HTTPs не представляется возможным.»

С уважением,

Кузнецов Александр

Тел. +7 (925) 261-82-10

От: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com>

Отправлено: 3 октября 2022 г. 11:34

Кому: 276-fz

Копия: Anton Nikitenkov

Тема: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Александр, добрый день.

Эксельку 2 раза в день по почте точно высылать не нужно.

Мы автоматически забираем с ваших серверов XML выгрузку.

Мой вопрос был возможно ли в ней добавить в блок content blockType = "domain"

В блоке

```
<content id="1202" includeTime="2013-12-01T10:00:05" blockType="domain" entryType="2"
hash="099B06DE7F7B1F61BD10E817704FE809">
  <decision date="2013-12-01" number="9" org="Мосгорсуд"/>
  <url><![CDATA[http://site2.com/page1.php]]></url>
  <url><![CDATA[http://site2.com/page2.php]]></url>
  <url><![CDATA[http://site2.com/page3.php]]></url>
  <domain><![CDATA[site2.com]]></domain>
</content>
```

Так мы будем видеть какие домены нужно блокировать, с нашей стороны все заработает.

Блокировать просто все домены которые есть в списке можно но среди них встречаются популярные.

Например если с вашей стороны будет заблокирован ролик на Youtube – весь домен попадет в блокировку. Мы получим много обращений в саппорт от пользователей.

Посмотрите пожалуйста можете ли доработать атрибут с вашей стороны.

С уважением,

Павел

Pavel Lastochkin | Product Manager | B2C Products | Kaspersky Lab

From: 276-fz <276-fz@rkn.gov.ru>

Sent: Friday, September 30, 2022 12:56 PM

To: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com>

Cc: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com>

Subject: Re: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Добрый день!

Направляем список URL-адресов с протоколом HTTPs и их доменами.

Указанный файл можем направлять в ежедневном формате утром и вечером.

С уважением,
Кузнецов Александр

От: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Отправлено: 23 сентября 2022 г. 14:58
Кому: 276-fz
Копия: Anton Nikitenkov
Тема: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Александр, добрый день.

Да это 15 HTTPS URL, которые мы сейчас не блокируем, потому что не можем технически разобрать HTTPS трафик. Мой вопрос в письме ниже – возможно ли с вашей стороны добавить эти домены в общий список доменов которые нужно блокировать, тогда все заработает.

С уважением,
Павел

Pavel Lastochkin | Product Manager | B2C Products | Kaspersky Lab

From: 276-fz <276-fz@rkn.gov.ru> >
Sent: Friday, September 23, 2022 12:57 PM
To: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Cc: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com> >
Subject: Re: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Добрый день!

На текущий момент выявлено 15 URL-адресов с протоколом https, доступ к которым не ограничивается, список ресурсов направляется во вложении. Все они находятся в блок-листе РКН и в выгрузке для VPN-сервисов. Напоминаем, что ранее в Ваш адрес направлялось письмо с информацией о возможности фильтрации URL-адресов с протоколом https по домену.

С уважением,
Кузнецов Александр

От: 276-fz
Отправлено: 16 сентября 2022 г. 12:01
Кому: Pavel Lastochkin
Копия: Anton Nikitenkov
Тема: Re: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Добрый день!

Выгрузка для VPN-сервисов содержит информацию о домене URL-адресов для протоколов http и https, например - <url><![CDATA[https://vulkan-platina.xyz/game/hall]]></url><domain><![CDATA[vulkan-platina.xyz]]></domain>. Для ограничения доступа к URL-адресам с протоколом https можете использовать информацию о доменах, содержащихся в выгрузке для VPN-сервисов.

На текущий момент выявлено 9 URL-адресов с протоколом https, доступ к которым не ограничивается, список ресурсов направляется во вложении. Все они находятся в блок-листе РКН и в выгрузке для VPN-сервисов.

С уважением,
Кузнецов Александр

От: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Отправлено: 13 сентября 2022 г. 12:12
Кому: 276-fz
Копия: Anton Nikitenkov
Тема: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Александр, добрый день!

Для https соединения, URL передается в зашифрованном виде, поэтому такую блокировку не может сделать никто из провайдеров.

Вы можете на своей стороне добавлять такие домены в список заблокированных?

С уважением,
Павел

Pavel Lastochkin | Product Manager | B2C Products | Kaspersky Lab

From: 276-fz <276-fz@rkn.gov.ru> >
Sent: Thursday, September 8, 2022 9:59 AM
To: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Cc: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com> >
Subject: Re: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Добрый день!

Поскольку фильтрация противоправных ресурсов по URL с протоколом HTTPs невозможна на Вашей стороне, можете осуществлять фильтрацию ресурсов с типом блокировки по URL (протокол HTTPs) по домену.

*С уважением,
Кузнецов Александр*

От: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Отправлено: 26 августа 2022 г. 19:12
Кому: 276-fz
Копия: Anton Nikitenkov
Тема: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Александр, добрый день!

При установке https соединения, URL передается в зашифрованном виде, поэтому алгоритмически невозможно реализовать фильтрацию по HTTPs урлам.

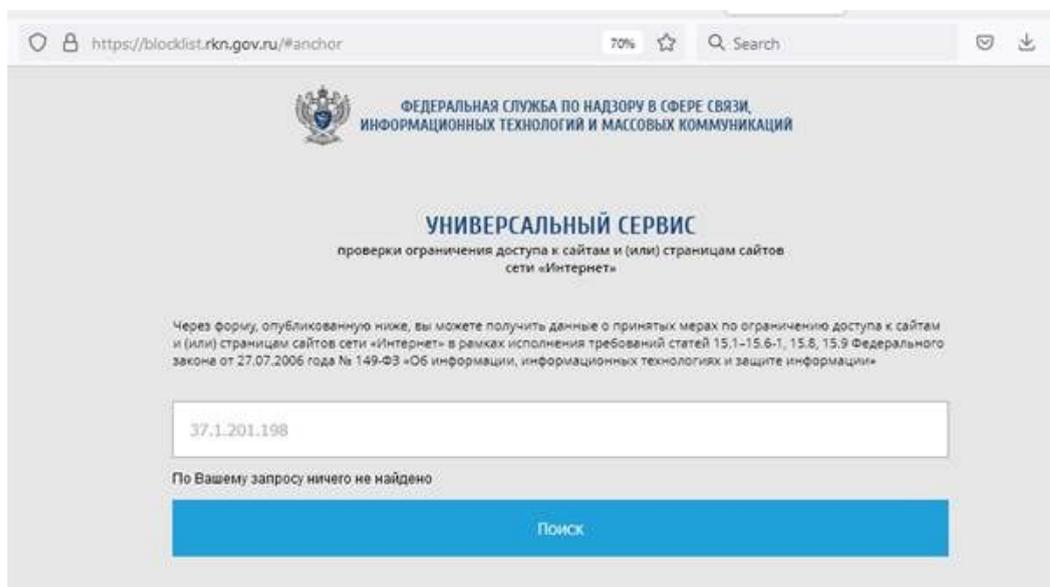
Все https открылись, так как этих базовых доменов в актуальном блеклисте нет.

Алгоритм блокировки по IP:

1. получаем список IP для блокировок из ФГИС
2. когда пользователь пытается установить соединение к какому-то IP, проверяем есть ли IP в выгрузке.
3. если IP есть в выгрузке, то разрываем соединение

По списку проверили, IP либо блокируется, либо его нет в актуальном списке. Пример блокировки во вложении. Тестирование провели на сборке 21.3.10.391 (j).

Пример отсутствия в реестре:



С уважением, Павел

Pavel Lastochkin | Product Manager | B2C Products | Kaspersky Lab

From: 276-fz <276-fz@rkn.gov.ru> >
Sent: Friday, August 26, 2022 12:52 PM
To: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com> >
Cc: Pavel Lastochkin <Pavel.Lastochkin@kaspersky.com> >
Subject: Re: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Антон, добрый день!

Направляю список с примером ресурсов, по которым блокировка не осуществляется.

Версия приложения – 21.3.10.391 (j).

Просим уточнить с чем связаны технические особенности, из-за которых невозможно обеспечить ограничение доступа к ресурсам по HTTPS URLs.

Помимо этого, просим сообщить принцип, по которому Вы ограничиваете доступ к IP-адресам.

С уважением,

Кузнецов Александр

От: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com> >
Отправлено: 25 августа 2022 г. 19:36
Кому: 276-fz
Копия: Pavel Lastochkin
Тема: RE: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Александр, добрый день.

Мы проверили работоспособность наших систем. И по нашему мониторингу, и по итогам тестирования – мы блокируем всё по списку, как и делали ранее.

Мы блокируем по вашему списку IP-адреса, домены, HTTP URLs.

HTTPS URLs блокировать нет технической возможности.

Можете, пожалуйста, уточнить дополнительную информацию для воспроизведения вашего сценария тестирования на нашей стороне:

- какие именно ресурсы не блокируются
- какая версия приложения использовалась вами

P.S. Заменяю список коллег в копии на актуальный.

2/8/2023

Regards,
Anton Nikitenkov | Senior Product Manager | Kaspersky Lab

From: 276-fz <276-fz@rkn.gov.ru >
Sent: Thursday, August 25, 2022 10:24 AM
To: Anton Nikitenkov <Anton.Nikitenkov@kaspersky.com >; Eldar Kononov <Eldar.Kononov@kaspersky.com >; Andrey Yarnikh <Andrey.Yarnikh@kaspersky.com >; Dmitry Momotov <Dmitry.Momotov@kaspersky.com >
Subject: Реализация статьи 15.8 Федерального закона № 149-ФЗ

Caution: This is an external email. Be cautious while opening links or attachments.

Коллеги, добрый день!

Роскомнадзором в рамках реализации статьи 15.8 Федерального закона № 149-ФЗ проводятся выборочные проверки Kaspersky Secure Connection на предмет фильтрации выгрузки.

На данный момент мы видим, что доступ к большей части URL и IP-адресам не ограничен.

Можете ли прокомментировать ситуацию, фильтрация по указанным типам работает?

Если у Вас имеются какие-либо технические особенности, в виду которых блокировка по URL и IP-адресам невозможна, просим уточнить и сообщить детали.

*С уважением,
Кузнецов Александр*