|  |  |
| --- | --- |
|  |  |

**Техническое задание**

**На систему защиты от продвинутых атак и интеллектуальной собственности**

1. ОБЩИЕ СВЕДЕНИЯ

Настоящее техническое задание содержит требования к программному обеспечению, направленному на защиту:

* + Корпоративной почты от сложных и продвинутых атак, а также от спама, фишинга и вредоносного ПО;
	+ Объектов исключительных прав Заказчика в сети Интернет посредством осуществления мониторинга, анализа и реагирования на предмет наличия признаков интернет-мошенничества с незаконным использованием средств индивидуализации (далее – бренд), включая товарные знаки, оказывающих негативное влияние на Заказчика.

Поставщиком программного обеспечения по настоящему Техническому заданию понимается правообладатель программного обеспечения (Лицензиар) или лицо, которое наделено правом заключения сублицензионного договора о передаче неисключительного права использования программного обеспечения сублицензиату.

1. ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ
	1. Требования к веб-интерфейсу
		1. Программное обеспечение должно обладать единым веб-интерфейсом.
		2. Доступ пользователей к Системе должен осуществляться с использованием протокола HTTPS, на основе ролевой модели, в соответствии с назначенными для каждой роли привилегиями.
	2. Требования к анализу
		1. Программное обеспечение должно проводить сигнатурный анализ с собственными сигнатурами с целью максимизации количества обнаруженных нарушений.
		2. Программное обеспечение должно иметь собственную систему оценки (математическую модель) уровня риска для соответствующих найденных ресурсов с нарушениями с целью формирования приоритетов для реагирования.
		3. Работоспособность программного обеспечения по настоящему техническому заданию должна осуществляться в режиме 24 х 7 х 365.
		4. Поставщик программного обеспечения при передаче неисключительного права использования программного обеспечения должен согласовать с Заказчиком список ответственных лиц с указанием контактных данных, электронную почту для последующей коммуникации с представителем клиентского сервиса по вопросам работы программного обеспечения и согласования дальнейших действий в нестандартных случаях.
	3. Состав и требования, предъявляемые к отчетной документации автоматически формируемой и выгружаемой посредством программного обеспечения
		1. Оперативные отчеты формируются по результатам обнаружения Нарушения в сроки, установленные настоящим техническим заданием (в зависимости от типа выявленного факта неправомерного использования объекта интеллектуальной собственности (далее – нарушение).
		2. Совокупные отчеты формируются один раз за отчетный период (ежемесячно).
		3. Все отчетные документы должны составляться на основе собранной, накопленной и проанализированной программным обеспечением информации об исследуемых и устраненных нарушениях и должны включать следующую информацию:
	* дата и время обнаружения нарушения;
	* ссылки на нарушения (url, описание контента и прочая информация);
	* анализ нарушения (включая описание причин, на основании которых сделан вывод о том, что обнаруженное является нарушением);
	* результаты реагирования;
	* динамику выявленных нарушений;
	* итоговые показатели эффективности в виде статистических данных, графиков и таблиц.
		1. Обмен информацией по работе программного обеспечения и согласование дальнейших действий по оперативным отчетам осуществляется по электронной почте либо через веб-интерфейс программного обеспечения.
2. Требование к подсистеме защиты корпоративной почты
	1. Общие требования
		1. Подсистема должна выявлять вредоносные программы, инструменты и методы проведения атак, реализуя следующие подходы:
	* выявление вредоносных файлов, поступающих через систему электронной почты, методом поведенческого анализа в ферме специально подготовленных виртуальных машин;
	* проверка заголовков письма, а также ссылок и вложений внутри на предмет социальной инженерии или вредоносной активности;
	* проверка электронных сообщений и выявление спам-рассылок и BEC-атак;
	* применение настраиваемых политик фильтрации почтовых писем для снижения рисков получения нежелательных рассылок и/или вредоносного контента.
		1. Подсистема должна реализовывать поведенческий анализ потенциально вредоносных файлов в изолированной среде для эффективного обнаружения ранее неизвестных угроз.
		2. Подсистема должна обеспечивать блокировку электронных писем, содержащих вредоносное программное обеспечение в виде ссылок на скачивание файла, либо вложения.
		3. Подсистема должна реализовывать статический и эвристический анализ электронных писем на предмет их принадлежности к нежелательным рассылкам, рассылкам с использованием методов социальной инженерии, в том числе атаки, реализованные путем компрометации корпоративной почты.
		4. Подсистема должна обеспечивать возможность блокировки электронных писем, относящихся к нежелательным рассылкам, рассылкам с использованием методов социальной инженерии, в том числе атак, реализованных путем компрометации корпоративной почты.
	1. Функциональные требования

**Требования к централизованному управлению**

* + 1. Подсистема должна обладать возможностью для автоматической и ручной корреляции событий информационной безопасности в единую сущность.
		2. Пользовательский интерфейс должен быть реализован в формате WEB-приложения с доступом по протоколу HTTP с возможностью шифрования трафика с использованием любого современного веб-браузера (на основе Chromium и подобных). Пользовательский интерфейс должен предоставлять доступ к регистрируемой информации с возможностью корреляции записей, поиска и построения статистических отчетов.
		3. Пользовательский интерфейс должен предоставлять возможность настройки почтовых уведомлений для пользователей системы для следующих случаев:
	+ появление новых событий информационной безопасности или новых связанных сущностей таких событий;
	+ изменение статуса событий информационной безопасности или связанных сущностей таких событий;
	+ информация об обновлениях системы;
	+ взаимодействие с центрами мониторинга и реагирования.
		1. Подсистема должна иметь возможность настройки почтовых уведомлений для получателей почтовых сообщений, если такие сообщения были заблокированы.
		2. Подсистема должна иметь необходимый функционал для передачи телеметрии и информации о регистрируемых событиях через механизм API для интеграции с другими решениями Заказчика.
		3. Подсистема должна иметь возможность осуществления автоматического поиска угроз, опираясь на тактики, техники и процедуры (TTP), полученные от служб киберразведки Исполнителя. Автоматический поиск угроз осуществляется через ретроспективный анализ следующих данных:
	+ проанализированные ранее файлы;
	+ проанализированные почтовые сообщения.

**Требования к анализу почтовых сообщений**

* + 1. Подсистема должна поддерживать работу в качестве первого on-cloud шлюза для входящей почты путем изменения MX-записей и перенаправления почтового потока в инфраструктуру разработчика для анализа и принятия решения о блокировке в подсистеме анализа почтовых сообщений;
		2. Подсистема должна обеспечивать непрерывный анализ почтовых сообщений для 4 000 активных почтовых ящиков.
		3. Подсистема должна предоставлять возможность для настройки почтовых маршрутов с указанием приоритетности и метрик значимости серверов, необходимых для балансировки нагрузки и распределения почтового потока между серверами.
		4. Подсистема должна осуществлять отправку почтовых сообщений по заданным почтовым маршрутам по результатам анализа, если сообщение признано безопасным, и применения всех заданных политик фильтрации.
		5. Подсистема должна предоставлять возможность для формирования белых списков, исключающих индикаторы из анализа, по следующим параметрам:
	+ email-адреса;
	+ URLs;
	+ контрольной суммы;
	+ IP адреса;
	+ MX-записи домена;
	+ тема письма.
		1. Подсистема должна включать в себя функционал для поведенческого анализа файлов в ферме специально подготовленных виртуальных машин в инфраструктуре сервис-провайдера.
		2. Подсистема должна проводить статический и эвристический анализ контента письма и его заголовков, а также ссылок внутри на предмет социальной инженерии, включая BEC-атаки и спам-рассылки, и предоставлять отчет с указанием перечня сработавших правил.
		3. Подсистема должна предоставлять возможность применять настраиваемые политики фильтрации почтовых писем для снижения рисков получения нежелательных рассылок и/или вредоносного контента.
		4. Подсистема должна предоставлять возможность настройки политики проверки форматов содержимого по следующим критериям:
		file\_name, file\_magic, url, recipient, sender, spf, dkim, dmark.
		5. Подсистема должна предоставлять возможность настройки политики действий с непроверенным контентом, включающим в себя зашифрованные архивы и недоступные ссылки.
		6. Подсистема должна предоставлять возможность добавления пользовательских YARA правил и настройки политики действий на основе их срабатывания.
		7. Подсистема должна предоставлять возможность принудительной отправки заблокированных почтовых сообщений получателю, указанному в заголовках письма.
		8. Подсистема должна предоставлять возможность принудительной отправки заблокированных почтовых сообщений на заданный администратором системы адрес.
		9. Подсистема должна предоставлять и реализовывать с помощью панели централизованного управления возможность представления технических заголовков письма и структуры почтового сообщения в виде графа.
		10. Подсистема должна выявлять поведенческие маркеры.
		11. Подсистема должна использовать элементы машинного обучения.
		12. Подсистема должна реализовывать анализ файлов в изолированной среде с использованием русифицированного образа ОС Windows.
		13. Архитектура подсистемы должна реализовывать возможность гибкого горизонтального масштабирования для наращивания производительности в случае необходимости.
		14. Подсистема должна предоставлять возможность анализа файлов до 100 Мб.
		15. Подсистема поведенческого анализа должна осуществлять анализ потенциально вредоносных файлов следующих расширений в изолированной среде: 7z, ace, ar, arj, bat, bz2, bzip2, cab, cmd, com, cpl, csv, doc, docm, docx, dot, dotm, dotx, eml, exe,gz, gzip, hta, htm, html, iso, jar, js, jse, lnk, lz, lzh, lzma, lzo, mht, msi, pdf, potm, potx, pps, ppsm, ppsx, ppt, pptm, pptx, ps1, rar, ref, rtf, scr, svg, tar, taz, tb2, tbz, tbz2, tgz, tlz, txz, tzo, url, uue, vbe, vbs, wsf, xar, xls, xlsm, xlsx, xml, xz, z, zip и др.
		16. Подсистема должна осуществлять анализ потенциально вредоносных файлов в изолированной среде с возможностью определения следующих типов файлов по содержимому для эффективного детектирования ранее неизвестных угроз:
	+ Android application;
	+ Архив;
	+ MS Windows HTMLHelp;
	+ CPGZ-file;
	+ CPIO-file;
	+ Control Panel File;
	+ DLL-file;
	+ EML-file;
	+ Исполняемый файл Windows;
	+ HTML Application;
	+ HTML-file;
	+ Java Application;
	+ JS-script;
	+ Ярлык;
	+ MCL-script;
	+ Windows Installer file;
	+ PDF-file;
	+ PowerShell script;
	+ Python-script;
	+ Файл реестра.
		1. Подсистема должна позволять загружать файлы в web-интерфейсе на анализ в ручном режиме, в том числе с возможностью задать параметры виртуализации и анализа.
		2. Подсистема должна осуществлять поведенческий анализ архивов с паролем.
		3. Подсистема должна обеспечивать поиск и подбор паролей из анализируемого контекста, а именно:
	+ содержимое и заголовки почтового сообщения, содержащего зашифрованный архив;
	+ контекст писем, предшествующих или последующих по отношению к письму, содержащему зашифрованный архив;
	+ все вложенные файлы анализируемого письма, включая метаданные файла;
	+ все файлы, скачиваемые по ссылкам, указанным в анализируемом письме или ссылкам, расположенным во вложенных файлах, включая метаданные файла;
	+ настраиваемый словарь возможных паролей;
	+ предустановленный в систему словарь паролей.
		1. Подсистема должна иметь следующие методы анализа потенциально вредоносного программного обеспечения в виртуальной среде:
	+ контроль событий операционной системы в процессе эмуляции исполнения файла должен выполняться на уровне ОС;
	+ должен осуществляться статический сигнатурный анализ файла;
	+ должно осуществляться автоматическое обнаружение и противодействие техникам обхода систем поведенческого анализа (VMEvasion, Sandbox-evasion).
		1. Подсистема по итогу анализа должна формировать отчет, содержащий следующие элементы:
	+ перечень процессов, зафиксированных на виртуальной машине во время проведения анализа в виде дерева и графа;
	+ внутренняя структура анализируемого файла в виде дерева;
	+ данные о сетевой активности файла во время анализа с разделением по протоколам L3-L7 и возможностью скачать полный снимок (копия) сетевого трафика в формате pcap;
	+ детализированное централизованное представление результата работы каждого процесса, включая данные о взаимодействии на уровне реестра, файловой системы, сетевой активности, мьютексах, а также метаданные самого процесса и перечень относящихся к этому процессу поведенческих и статических правил;
	+ детализированное централизованное представление информации о файлах, проанализированных системой, а также файлов, создаваемых в результате поведенческого анализа и/или извлеченных из памяти процессов, включая: метаданные, взаимодействие с процессами и перечень относящихся к этому файлу поведенческих и статических правил;
	+ фрагменты памяти процессов, созданных в результате проведения поведенческого анализа;
	+ перечень сработавших поведенческих и статических правил с указанием тактик и техник по классификации MITRE, а также индикаторами сработки, извлеченными в результате поведенческого анализа;
	+ MITRE ATT&CK matrix построенную для проанализированного файла с указанием задействованных TTPs и возможностью её экспорта в формате json;
	+ запись экрана виртуальной машины за период проведения поведенческого анализа;
	+ перечень параметров анализа.
		1. Подсистема должна обладать функциональностью обнаружения и извлечения конфигурационных файлов ВПО с указанием перечня командных центров, способов и мест закрепления на системе, параметров работы.
		2. Подсистема должна предоставлять атрибуцию проанализированных объектов к известным инструментам, группировкам и/или семействам вредоносного ПО.
		3. Подсистема должна позволять экспортировать анализируемые файлы, а также любые файловые объекты, относящиеся к проведенному анализу, в защищенном виде для их последующего анализа сторонними экспертами.
		4. Подсистема должна поддерживать операционные системы: Windows XP, Windows 7 и Windows 10 в двух вариантах разрядности – x64/x86, Android 7.
		5. Подсистема должна поддерживать два варианта локализации: русский и английский.
		6. Подсистема должна предоставлять возможность изменения маршрута для вывода трафика из виртуальных машин внутри подсистемы поведенческого анализа.
		7. Подсистема должна предоставлять возможность кастомизации виртуальных машин в web-интерфейсе путем добавления настроек для виртуальных машин: домена, имени компьютера, имени пользователя.
		8. Подсистема должна реализовывать следующую функциональность:
	+ автоматический подбор конфигурации виртуальной машины для анализа экземпляра вредоносного ПО;
	+ эмуляция пользовательской активности (движения мыши, нажатие клавиш, переключение между окнами);
	+ технология компьютерного зрения;
	+ извлечение и запуск дополнительных команд из реестра;
	+ опция поддельного SMTP-сервера для проведения анализа;
	+ включение Mitmproxy.

**Требования к сервисному сопровождению системы анализа почтовых сообщений**

Предоставление услуг по мониторингу должно осуществляться в режиме 24 часа в сутки, 7 дней в неделю и 365 (366 для високосного года) дней в году, без выходных и праздников.

Специалисты CERT Исполнителя должны реализовывать функции SOC и анализировать информацию, передаваемую дочерними подсистемами в ПЦУ, оповещать работников Заказчика о выявленных инцидентах ИБ не позднее 2-х часов с момента возникновения критического события. Подробные условия описаны в Соглашении об Уровне Сервиса.

Техническая поддержка решения должна быть включена в пакет поставки и осуществляться в объеме, соответствующем тарифу.

База решающих правил должна создаваться на основе следующих процессов, организованных производителем базы данных, для эффективного детектирования угроз, распространяемых на территории Российской Федерации:

1. работы действующей криминалистической лаборатории, осуществляющей криминалистические экспертизы по высокотехнологичным преступлениям на территории Российской Федерации;

2. работы автоматизированных средств сбора и анализа вредоносного ПО, распространяемого на территории Российской Федерации;

3. получения разведывательной информации о действиях преступных групп через мониторинг преступных сообществ и проводимое наблюдение за их действиями.

1. Требования к подсистеме защиты исключительных прав Заказчика в сети Интернет
	1. Описание подсистемы

Подсистема включает в себя функционал для мониторинга случаев незаконного использования бренда Заказчика, анализа, выявления нарушений и принятия мер для их устранения.

Целью запрашиваемой услуги является обеспечение защиты бренда/товарного знака Заказчика, неправомерное использование которого может оказывать негативное влияние на Заказчика, путем обнаружения в сети Интернет нарушений, связанных с использованием бренда/ товарного знака, и Целью запрашиваемой услуги является обеспечение защиты бренда/товарного знака Заказчика, неправомерное использование которого может оказывать негативное влияние на Заказчика, путем обнаружения в сети Интернет нарушений, связанных с использованием бренда/ товарного знака, и осуществления мер по блокировке, ограничению доступа, удалению упоминаний и прочих действий, направленных на устранение нарушения, связанного с неправомерным использованием бренда (далее – нейтрализация) вредоносных ресурсов или вывода мошеннического и вредоносного содержимого или информационного наполнения ресурса в сети интернет (далее - контент) из прямого публичного доступа через сеть Интернет (в случае наличия легитимной возможности).

В рамках предоставляемой услуги должны быть реализованы следующие задачи:

* + Выявление, анализ и нейтрализация контента, содержащего вредоносный код, признаки мошенничества, а также нарушения, связанные с неправомерным использованием бренда/ товарного знака, предоставлением фиктивных услуг от лица Заказчика;
	+ Нейтрализация Нарушений в социальных сетях;
	+ Выявление и нейтрализация мошеннических приложений в официальных и неофициальных интернет-магазинах приложений, незаконно использующих бренд Заказчика.
	1. Требования к веб-интерфейсу

Клиентский веб-интерфейс должен содержать и предоставлять:

* + авторизацию в личном кабинете с помощью почты и заданного пароля;
	+ контрольную панель со сводной информацией об обработанных/выявленных нарушениях;
	+ подробную информацию о каждом выявленном нарушении;
	+ возможность согласования выявленных нарушений при реализации функций автоматического мониторинга и реагирования;
	+ возможность фильтрации по разным типам нарушений;
	+ возможность отслеживания изменений по нарушениям в календаре событий каждого из них;
	+ возможность автоматической выгрузки отчетов в форматах .pdf и .xlsx;
	+ возможность анализа ресурсов при помощи построенного сетевого графа связей.
	1. Требования к функционалу

На основе заданных критериев программное обеспечение должно выявлять и фиксировать Нарушения. После установления и подтверждения со стороны Заказчика факта незаконного использования его бренда/товарного знака на веб-страницах, программное обеспечение должно в автоматическом режиме отправлять администратору веб-сайта претензию. При отсутствии ответа/в случае неустранения администратором Нарушения, претензии направляются хостинг-провайдеру и регистратору доменного имени данного веб-сайта.

Исполнитель должен иметь систему анализа и расследования киберпреступлений, выявления готовящихся атак, фишинга и онлайн мошенничества, а также на регулярной основе производить обогащение программного обеспечения сведениями из данной системы.

Программное обеспечение должно обладать следующим функционалом:

* 1. Мониторинг
		1. Сбор информации о зловредных ресурсах в сети Интернет (Фишинг-сайты, Фальшивые сайты, Сайты, причастные к мошенническим кампаниям, использующие бренды Заказчика).
		2. Мониторинг ключевых слов во всевозможных написаниях, а также слов, созвучных и схожих по написанию с целью обнаружения зловредных ресурсов.
		3. Выявление ресурсов в сети Интернет, неправомерно использующих бренд Заказчика.
		4. Возможность собирать следующие типы информации:
			+ Скриншоты ресурса
			+ Скриншоты рекламы (при наличии)
			+ HTML файлы
			+ Информация про инфраструктуру сайта
			+ Источники трафика
			+ Другие параметры доменных имен
		5. Мониторинг осуществляется по следующим источникам:
			+ база доменных имен
			+ базы фишинговых и мошеннических ресурсов
			+ социальные сети
			+ поисковые системы
			+ официальные и неофициальные магазины мобильных приложений
			+ контекстная реклама
			+ торговые площадки и доски объявлений
			+ телеграм-каналы
			+ теневые форумы, Darknet, специализированные форумы и группы в мессенджерах.
			+ ресурсы для обмена данными (в том числе логины, пароли, фрагменты исходного кода и др.), такие как github.com, pastebin.com и др.
	2. Противодействие мошенническим веб-сайтам
		1. Возможность по нейтрализации вредоносного ресурса или мошеннического и вредоносного контента.
		2. Возможность заказать совокупный отчет о выявленных в отчетном периоде Нарушениях, статусе их нейтрализации.
		3. Возможность проводить маркировку найденных ресурсов для оперативного автоматизированного выявления нелегитимного использования измененных, дополненных объектов интеллектуальной собственности Заказчика.
	3. Мониторинг и выявление сайтов, которые неправомерно реализуют товар/услуги Заказчика
		1. Выявление осуществляется по следующим типам нарушений:
			+ мошеннические сайты
			+ сайты-клоны
			+ фишинговые ресурсы
			+ введение в заблуждение о партнерстве
			+ поддельные мобильные приложения
			+ поддельные аккаунты и группы в социальных сетях
			+ поддельные аккаунты и группы в мессенджерах
		2. Возможность сбора информации о ресурсах в сети Интернет, которые занимаются незаконной реализацией услуг от имени Заказчика.
		3. Мониторинг ключевых слов во всевозможных написаниях, а также слов, созвучных и схожих по написанию с целью обнаружения ресурсов, направленные на незаконную реализацию услуг от имени Заказчика.
		4. Возможность отображения связей ресурсов посредством графового анализа с целью определения полноценной инфраструктуры злоумышленника и аффилированных друг с другом найденных сайтов на основе различных критериев.
	4. Анализ информации и нейтрализация угроз из социальных сетей
		1. Выявление незаконного использования бренда Заказчика, согласно ключевым словам на следующих типах ресурсов:
* Социальные сети;
* Публичные чаты и каналы Telegram, которые используют бренд Заказчика.
	+ 1. Возможность по нейтрализации ресурса или по выводу мошеннического и вредоносного контента из прямого публичного доступа через сеть Интернет.
		2. Возможность выгрузки отчета о выявленных в отчетном периоде Нарушениях, статусе их нейтрализации.
	1. Мониторинг мобильных приложений
		1. Функционал по мониторингу интернет-магазинов мобильных приложений для IOS, Android, а также неофициальных Интернет-ресурсов, распространяющих мобильные приложения.
		2. Возможность выгрузить отчет по итогам выявленных приложений.
		3. Возможность оперативного удаления мошеннических приложений из интернет-магазинов.
		4. Возможность автоматической выгрузки отчета о выявленных в отчетном периоде мошеннических приложениях, статусе их нейтрализации.
		5. Возможность проведения мониторинга с использованием различных геолокационных и временных параметров, аккаунтов, операционных систем.
	2. Мониторинг торговых площадок и досок объявлений
		1. Мониторинг использования товарного знака в мошеннических объявлениях на торговых площадках и досках объявлений.
		2. Возможность по нейтрализации мошеннического объявления с использованием товарного знака Заказчика или по выводу мошеннического и вредоносного контента из прямого публичного доступа через сеть Интернет.
		3. Возможность выгрузить отчет о выявленных нарушениях, статусе их нейтрализации в отчетном периоде.
	3. Выявление утечек корпоративных логинов и паролей.
		1. Мониторинг теневых форумов и специализированных площадок с целью обнаружения утечек баз данных, содержащих логины и пароли.
		2. Предоставление информации об обнаруженных утечках.
		3. Возможность автоматической выгрузки файла с данными о выявленных утечках.
	4. Выявление конфиденциальной информации на ресурсах для обмена данными.
		1. Мониторинг общедоступных ресурсов (например, github.com, pastebin.com и другие) на предмет выявления записей, содержащих конфиденциальную информацию о Заказчике (логины, пароли фрагменты исходного кода и др.).
		2. Предоставление информации об обнаруженных утечках и источниках.
		3. Возможность автоматической выгрузки файла с данными о выявленных записях, содержащих конфиденциальную информацию о Заказчике.
	5. Анализ возможных угроз на специализированных форумах и в Darknet.
		1. Выявление и информирование Заказчика об информации на специализированных форумах, представляющую угрозу.
		2. Предоставление информации об обнаруженных утечках и источниках.
		3. Возможность автоматической выгрузки файла с данными о выявленных фактах упоминания бренда на форумах и специализированных площадках.
1. Требование к количеству лицензий и продолжительности предоставления услуги
	* 1. Срок оказания услуги должен составлять не менее 24 календарных месяцев с момента начала оказания услуги.
		2. Количество контролируемых электронных почтовых адресов, не менее:
			1. Для ПАО «Группа Ренессанс Страхование» – 3000 штук.
			2. Для ООО «СК „Ренессанс Жизнь“» – 1000 штук.
2. Требования к исполнителю
	* 1. Исполнитель должен иметь как минимум пять лет опыта и положительную репутацию в сфере информационной безопасности в вопросах решения задач мониторинга информации и защите объектов интеллектуальной собственности в сети Интернет.
		2. Исполнитель должен обладать компетенциями по досудебному устранению нарушений на ресурсах как в российских доменных зонах, так и за их пределами.
		3. Исполнитель должен иметь статус компетентной организации Координационного центра национального домена сети Интернет.
		4. Исполнитель должен иметь собственный центр реагирования на киберугрозы (CERT), аккредитованный в следующих организациях: КЦ (Координационный центр) Национального домена сети Интернет. CERT (Computer Emergency Response team) должен осуществлять свою работу в режиме 24x7x365.
		5. Исполнитель должен обладать действующей криминалистической лабораторией, осуществляющей криминалистические экспертизы по высокотехнологичным преступлениям на территории Российской Федерации.
		6. В штате Исполнителя должны числиться сотрудники с действующими сертификатами WIPO (Всемирной организации интеллектуальной собственности) со стажем работы у Исполнителя от года.