Приложение № 2
к приказу Фонда перспективных исследований
от «30» января 2019 г. № 10

Конкурсная документация

открытого конкурса Фонда перспективных исследований
на лучшее решение в области создания интеллектуальной технологии
поведенческого анализа сетевых устройств

1. Определения

Заявка – направленный организатору комплект документов в соответствии с требованиями настоящей Конкурсной документации.

Конкурс – открытый конкурс Фонда перспективных исследований на лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств.

Конкурсная комиссия – коллегиальный орган, создаваемый Организатором Конкурса, для выбора победителя (победителей) Конкурса.

Организатор – Фонд перспективных исследований. Техническим партнером в организации Конкурса является ЗАО «Перспективный мониторинг».

Регламент Конкурса – документ, определяющий этапы и сроки Конкурса, формат исходных данных и результатов, требования к программам (Приложение № 4 к настоящей Конкурсной документации).

Участник Конкурса – юридическое лицо независимо от организационно-правовой формы, являющееся резидентом Российской Федерации, созданное на территории Российской Федерации без участия иностранных граждан, иностранных или международных организаций (работа по выполнению конкурсных заданий проводится на территории Российской Федерации при непосредственном участии граждан Российской Федерации), подавшее Заявку.

Экспертная комиссия – коллегиальный орган, создаваемый Конкурсной комиссией из членов Конкурсной комиссии и приглашенных экспертов для оценки результатов участников каждого этапа Конкурса.

2. Общие положения

2.1. Конкурс проводится в два этапа:

первый этап – регистрация и обучение, построение предварительного рейтинга (проводится в заочной форме);

второй этап – подведение итогов (проводится в очной форме).

2.2. Конкурсная документация определяет порядок организации и проведения Конкурса, его информационное и методическое обеспечение, форму участия в Конкурсе и процедуру определения победителя (победителей).

2.3. Цель проведения Конкурса – выявление лучших отечественных коллективов и формирование эффективной кооперации для реализации проекта Фонда перспективных исследований по созданию технологии обнаружения и предупреждения компьютерных атак на объекты критической информационной инфраструктуры (далее – КИИ) на ранних стадиях их подготовки.

2.4. Основные задачи Конкурса:

- сопоставление отечественных технологий идентификации устройств в трафике и выявления сетевых атак в условиях отсутствия априорной информации;
- экспериментальная проверка программных реализаций алгоритмов идентификации устройств в трафике и выявления сетевых атак;
- выявление российских научных коллективов, способных проводить исследования инновационного характера в области создания интеллектуальных технологий анализа трафика, способных заменить человека-оператора при решении задач по картированию сегмента сети Интернет и защите отечественных ресурсов сети Интернет;
- повышение интереса научного сообщества к решению научно-технических задач в области анализа трафика;
- определение по итогам Конкурса победителя (победителей) и заключение с ним(и) договора о реализации научно-технического проекта Фонда перспективных исследований по созданию технологии обнаружения и предупреждения компьютерных атак на объекты КИИ на ранних стадиях их подготовки.

2.5. Конкурс предполагает участие в двух номинациях:

- Лучшее решение по идентификации устройств в трафике;
- Лучшее решение по превентивному выявлению сетевых атак.

2.6. Для проведения Конкурса приказом Фонда перспективных исследований создается Конкурсная комиссия (Комиссия), формируется и назначается ее состав и сроки функционирования.

2.6.1. Комиссия утверждает список участников второго этапа Конкурса путем оформления протокола заседания Комиссии.

2.6.2. Сроки проведения Конкурса могут быть изменены на основании решения Комиссии, оформленного протоколом заседания Комиссии.

2.6.3. Комиссия в соответствии с критериями, установленными в п. 3.8 настоящей Конкурсной документации, определяет победителя (победителей)

в номинациях «1. Лучшее решение по идентификации устройств в трафике» и «2. Лучшее решение по превентивному выявлению сетевых атак», с которым(и) подписывается соглашение (в соответствии с п. 6.2.1 настоящей Конкурсной документации) о подготовке документации на реализацию научно-технического проекта Фонда перспективных исследований по созданию технологии обнаружения и предупреждения компьютерных атак на объекты КИИ на ранних стадиях их подготовки.

2.7. Участие в Конкурсе является добровольным и бесплатным.

2.8. Организатор обязуется обеспечить осуществление аудио- и (или) видеозаписи процедуры заседания конкурсной комиссии.

3. Порядок организации и проведения Конкурса

3.1. Этапы Конкурса:
первый этап (отборочный);
второй этап (заключительный).

Таблица 1 – сроки проведения конкурса, предоставляемые документы и критерии отбора победителей

Этап	Сроки		Представляемые документы	Критерии отбора (пункты настоящей Конкурсной документации)
	начало	окончание		
1	04.02.2019	15.03.2019	Заявка на участие; предложение по решению конкурсной задачи	п. 3.4
2	18.03.2019	29.05.2019	Сопроводительная документация; анкета участника; презентация и демонстрация предложенного решения	п. 3.8

3.2. Объявление о проведении Конкурса и Конкурсная документация размещаются на официальном сайте Организатора http://fpi.gov.ru. Для того, чтобы принять участие в первом этапе Конкурса, необходимо направить скан-копию заявки на участие в Конкурсе (Приложение № 1 к настоящей Конкурсной документации) на электронную почту traffic@fpi.gov.ru, указав в теме письма «Конкурс ФПИ-2019-Т: регистрация». Возможна подача заявки на участие в Конкурсе в электронной форме на сайте Фонда «Сколково», размещенной по адресу https://cyberday.sk.ru/fpi_app/.

Считается, что Участник Конкурса принял участие в первом этапе Конкурса только после ответного подтверждения получения Организатором указанных в п. 3.2 настоящей Конкурсной документации документов, направленного на электронную почту Участника Конкурса.

3.3. Участие в первом этапе Конкурса предполагает:

3.3.1. Решение одной из двух конкурсных задач.

3.3.2. Разработку программного решения, реализующего алгоритмы решения конкурсных задач: идентификация устройств в трафике и превентивное выявление сетевых атак, детальное описание конкурсных задач приведено в разделе «Исходные данные и формат предоставляемых результатов» Регламента Конкурса (приложение № 4 к настоящей Конкурсной документации).

3.3.3. Предоставление доступа (физического либо удаленного) к исполняемым файлам, разработанным с целью решения конкурсных задач, и результатам работы программных решений в соответствии с Приложением № 2 к Конкурсной документации. Необходимо направить скан-копию заполненного предложения по решению задачи на электронную почту Организатора traffic@fpi.gov.ru.

3.4. Критерии отбора решений Участников Конкурса, представленных на первом этапе:

3.4.1. Наличие направленных Организатору результатов работы программных решений. Дата предоставления результатов работы программных решений указана в Регламенте Конкурса (приложение № 4 к настоящей Конкурсной документации).

3.4.2. Предоставление Организатору доступа к исполняемым файлам (п. 3.3.3 настоящей Конкурсной документации) и инструкции по воспроизведению результатов работы программных решений.

3.5. Участник Конкурса, который соответствует критериям, определенным в п. 3.4 настоящей Конкурсной документации, на основании решения Комиссии проходит во второй этап Конкурса.

3.6. В случае если Участник Конкурса не предоставил доступ к исполняемым файлам (п. 3.3.3 настоящей Конкурсной документации), по решению Конкурсной комиссии для него сохраняется возможность перейти в заключительный этап Конкурса, но при этом Участник Конкурса обязуется продемонстрировать работу программного решения очно.

3.7. Участие во втором этапе Конкурса предполагает:

3.7.1. Отбор участников, чьи решения соответствуют требованиям по результатам проверки воспроизводимости результатов (построение предварительного рейтинга). Предоставление доступа к необходимому ПО и помощь в воспроизведении результатов работы алгоритма являются обязанностями Участника Конкурса.

3.7.2. Соответствие минимальным требованиям производительности. Информация об ограничениях по производительности работы алгоритмов описана в разделе «Требования к программам» Регламента Конкурса (приложение № 4 к настоящей Конкурсной документации).

3.7.3. Воспроизводимость результатов на контрольных данных в рамках очной демонстрации работы программных решений.

3.7.4. Подготовку сопроводительной документации, описывающей реализованный алгоритм решения конкурсной задачи. При этом должны быть отмечены:

- основные достоинства и недостатки алгоритма;
- особенности применения и функциональные ограничения алгоритма;
- перспективы развития технологии;
- план развития проекта.

3.7.5. Подготовку анкеты проекта в соответствии с Приложением № 3 к Конкурсной документации. Необходимо направить скан-копию заполненной анкеты на электронную почту Организатора traffic@fpi.gov.ru.

3.7.6. Участие в научно-практическом семинаре с докладом Участника Конкурса. Целью семинара является обсуждение развития представленного на Конкурс демонстрационного образца в рамках выполнения научно-технического проекта Фонда перспективных исследований. Построение итогового рейтинга Участников Конкурса

3.8. Критерии Конкурсной комиссии выбора победителей Конкурса на втором (заключительном) этапе:

3.8.1. Решение одной или нескольких конкурсных задач.

3.8.2. Оценка качества работы решения Конкурсной и Экспертной комиссиями.

3.8.3. Научно-технический задел и потенциал коллектива Участника Конкурса.

3.8.4. Качество и производительность решения.

3.8.5. Возможности и перспективы усовершенствования демонстрационных образцов предлагаемой технологии.

3.8.6. Наличие в составе демонстрационного образца технологии, разработанного в рамках настоящего Конкурса, программного обеспечения, права на которое принадлежат третьим лицам.

3.8.7. Наличие потенциальных конкурентных преимуществ создаваемой технологии перед мировыми аналогами.

3.8.8. Качество проработки плана развития разработанного образца технологии.

3.9. По совокупности критериев, определенных в п. 3.8 настоящей Конкурсной документации, в ходе экспертизы по комплексной оценке решений Участников Конкурса Конкурсная комиссия принимает решение о выборе победителя (победителей) в номинациях согласно п. 2.5 настоящей Конкурсной документации.

3.10. На всех стадиях жизненного цикла разрабатываемой технологии Участники Конкурса обязуются не нарушать права и законные интересы третьих лиц.

4. Порядок предоставления данных

4.1. Исходные данные предоставляются Участникам Конкурса после выполнения условий п. 3.2 настоящей Конкурсной документации.

4.2. Предоставляемые исходные данные являются конфиденциальной информацией. Обработка и использование исходных данных ограничиваются решением задач, определенных Конкурсной документацией. Использование исходных данных в иных целях не допускается.

4.3. Организатор оставляет за собой право дополнять исходные данные в ходе всего Конкурса.

5. Подведение итогов и определение победителя (победителей) Конкурса

5.1. Результаты первого этапа Конкурса размещаются на официальном сайте Организатора http://fpi.gov.ru не позднее чем через 14 календарных дней со дня его завершения.

5.2. Организатор оставляет за собой право признать Конкурс несостоявшимся и досрочно завершить его на любом из проводимых этапов.

5.3. В случае, если Конкурс признан несостоявшимся, считается, что победитель (победители) отсутствуют.

6. Права победителя (победителей) Конкурса

6.1. Конкурсная комиссия посредством комплексной экспертизы качества решений и перспектив развития представленных технологий определяет победителя (победителей) Конкурса.

6.2. Если Конкурс признан состоявшимся и определен победитель (победители): между Фондом перспективных исследований и победителем (победителями) Конкурса в указанных в п. 2.5.3.1 настоящей Конкурсной документации номинациях, определенным(и) в соответствии с критериями п. 3.8 настоящей Конкурсной документации, в течение 14 календарных дней со дня размещения на сайте Фонда перспективных исследований http://fpi.gov.ru приказа Фонда о победителе (победителях) Конкурса, подписывается соглашение о подготовке документации на реализацию научно-технического проекта (его составных частей) Фонда перспективных исследований (цели и задачи проекта (его составных частей) будут представлены победителю (победителям) Конкурса)[1].

[1] В случае наличия нескольких победителей Фонд перспективных исследований оставляет за собой право сформировать состав кооперации исполнителей (из числа победителей) с определением головного.

Приложение № 1
к Конкурсной документации

Заявка на участие в открытом конкурсе Фонда перспективных исследований на лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств

(на фирменном бланке организации)

№ _____ «___» _____ 20__ г.

Изучив Конкурсную документацию,

_____

(фирменное наименование (для юридического лица), фамилия, имя, отчество (для физического лица))

в лице

_____

(наименование должности руководителя (уполномоченного лица) и его Ф.И.О.)

сообщает, что согласен исполнить все регламентированные ею условия и представляет следующие сведения:

№	Наименование	Сведения об участнике
1.	Полное наименование и сокращенное наименование (для юридического лица)/Ф.И.О. (для физического лица)	
2.	ИНН/КПП (для юридического лица)/ОГРН (для юридического лица)	
3.	Сведения о регистрации в ЕГРЮЛ (ЕГРИП) - дата и номер Свидетельства, кем выдано (для юридического лица)	
4.	Юридический/фактический адрес (адрес регистрации, адрес места фактического нахождения - для юридического лица; место жительства - для физического лица)	
5.	Должность, Ф.И.О. единоличного исполнительного органа юридического лица	
6.	Должность, Ф.И.О. лица, действующего на основании доверенности от имени участника Конкурса (в случае подписания документов лицом, действующим по доверенности)	
7.	Должность, Ф.И.О., контакты ответственного лица участника Конкурса (с указанием кода города)	
8.	Телефон/факс (с указанием кода города)	
9.	Адрес электронной почты	

_____ _____ (_____)

должность *подпись* *расшифровка*

м.п.

Приложение № 2
к Конкурсной документации

Предложение по решению задачи открытого конкурса Фонда перспективных исследований на лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств

(на фирменном бланке организации)

№ _____ «___» _____ 20__ г.

Изучив Конкурсную документацию,

_____

(фирменное наименование, сведения об организационно-правовой форме, о месте нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные, сведения о месте жительства (для физического лица)

в лице

_____

(наименование должности руководителя (уполномоченного лица) и его Ф.И.О.)

сообщает, что согласен исполнить все регламентированные ею условия и представляет следующие сведения:

1. Сведения об участнике:

1.1. Место нахождения (для юридического лица), место жительства (для физического лица): _____

1.2. Контактное лицо _____ телефон _____

2. Перечень прилагаемых материалов:

№	Наименование	Примечание
1.	Архив с исполняемыми файлами или ссылка доступа к исполняемому файлу	
2.	Дополнительное ПО, необходимое для запуска исполняемого файла или для доступа к исполняемому файлу	
3.	Пакет сопроводительной документации, описывающей реализованный алгоритм (в соответствии с пунктом 3.3.2 Конкурсной документации)	
4.	Результат работы алгоритма в соответствии с конкурсной задачей: 4.1. лучшее решение по идентификации устройств в трафике; 4.2. лучшее решение по превентивному выявлению сетевых атак	

Участник Конкурса
(уполномоченный представитель
на осуществление действий
от имени участника Конкурса) _____ (_____)

подпись *расшифровка*

Приложение № 3
к Конкурсной документации

Анкета Участника заключительного этапа открытого конкурса Фонда перспективных исследований на лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств

ОБЩАЯ ИНФОРМАЦИЯ

1. Наименование проекта (базовой технологии)

2. Наименование (Ф.И.О.) Заявителя

Если заявитель – юридическое лицо:
Полное фирменное наименование
Место нахождения
Почтовый адрес
Сайт в сети «Интернет»
ОГРН
ИНН
Телефон
Адрес электронной почты
Сайт в сети «Интернет»

3. Контактное лицо по проекту (лицо, заполнявшее анкету):
   a. Ф.И.О.;
   b. телефон;
   c. e-mail.

4. Номинация, к которой относится проект (можно выбрать от одной до двух номинаций):
   1. лучшее решение по идентификации устройств в трафике;
   2. лучшее решение по превентивному выявлению сетевых атак.

5. Краткое резюме проекта (5 предложений) с указанием имеющихся наработок и основных целей развития проекта.

ПРОБЛЕМА И РЕШЕНИЕ

6. Как проект решает описанные задачи (из раздела 4 данной Анкеты), в чем заключается инновационность подхода.

7. Опишите основные технологические и рыночные тренды в рассматриваемой отрасли.

ТЕХНОЛОГИЯ

8. Приведите описание базовой технологии.

9. Приведите описание технических характеристик базовой технологии.

10. Опишите научно-технический задел, имеющийся у заявителя и обеспечивающий решение поставленной задачи.

11. Укажите, при наличии, имеющие непосредственное отношение к проекту российские и (или) зарубежные научные публикации, патенты и (или) заявки на выдачу патента:
    a. …
    b. …

КОНКУРИРУЮЩИЕ РЕШЕНИЯ

12. Перечислите наиболее близкие аналоги решения на рынке и опишите, в чем заключается преимущество базовой технологии.

13. Перечислите научные группы, институты, компании, ведущие аналогичные или близкие разработки и опишите, в чем заключается преимущество базовой технологии.

РЕСУРСЫ

14. Получали ли Вы и (или) члены команды проекта гранты на данную или схожую тематику (даты, суммы, характер проектов, полученные результаты)?
15. Привлекалось ли венчурное и (или) иное финансирование (инвесторы, суммы, результаты)?
16. Информация об участии проекта в программах институтов развития (если да, то указать название института развития)

ЦЕЛИ И ЗАДАЧИ ПЕРСПЕКТИВНОГО ПРОЕКТА В РАЗВИТИЕ БАЗОВОЙ ТЕХНОЛОГИИ

17. Укажите задачи, предлагаемых к решению в рамках перспективного проекта.
18. Текущий статус перспективного проекта (какие результаты уже достигнуты и чем они подтверждены).
19. Предполагаемый срок реализации перспективного проекта.
20. Ориентировочная стоимость перспективного проекта.
21. Опишите ключевые цели перспективного проекта и ориентировочный срок их достижения:
    a. …
    b. …
    c. …

22. Описание ожидаемого научно-технического результата перспективного проекта.
23. Обоснование выбора технических решений (принципов, подходов), заявленных параметров, технических характеристик.
24. Обобщенный план реализации перспективного проекта.

Участник Конкурса
(уполномоченный представитель
на осуществление действий
от имени Участника Конкурса) _____ (_____)
подпись *расшифровка*

Приложение № 4
к Конкурсной документации

Регламент открытого конкурса на лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств

1. Этапы

1. Отборочный этап (заочный): 04 февраля 2019 года – 15 марта 2019 года.
2. Заключительный этап (очный): 18 марта 2019 года – 29 мая 2019 года.

2. Ключевые даты

04 февраля 2019 года – старт Конкурса и начало регистрации, предоставление исходных данных по запросу Участника Конкурса (в соответствии с пунктом 3.2 Конкурсной документации).

23:59 (по московскому времени) 15 марта 2019 года – окончание приема финальных версий решений конкурсных задач и доступа к исполняемым файлам, разработанным с целью решения конкурсных задач. Участник Конкурса также должен прислать инструкции по запуску программы.

18 марта 2019 года – 01 мая 2019 года – анализ результатов работы алгоритмов, экспертная оценка результатов и выделение группы лидеров для заключительного очного этапа.

01 мая 2019 года – 29 мая 2019 года – заключительный очный этап.

29 мая 2019 года – определение победителя (победителей).

3. Исходные данные и формат предоставляемых результатов

Решение задач по идентификации устройств в трафике (задача картирования сегмента сети Интернет) и превентивному выявлению сетевых атак (задача защиты отечественных ресурсов сети Интернет) осуществляется на основании предоставленных Организатором исходных данных.

3.1. Исходные данные

Исходные данные предоставляются отдельно для каждой из номинаций:

- Лучшее решение по идентификации устройств в трафике;
- Лучшее решение по превентивному выявлению сетевых атак.

3.1.1. Исходные данные для задачи идентификации устройств в трафике

Исходные данные содержат дамп трафика.

Исходные данные разбиты на две выборки: *обучающую и контрольную* (далее Train_1 и Test_1 соответственно).

Обучающая выборка Train_1 включает в себя дамп трафика и экспертную разметку трафика.

Дамп трафика представлен в виде набора pcap-файлов. Для каждого класса устройств предоставляется 50 файлов. Общее количество пакетов в трафике для каждого класса - более 10 000.

Экспертная разметка представляется в виде образцов трафика и классов устройств, сгенерировавших тот или иной трафик, и содержится в csv-файле *devices_train.csv*. В каждой строке файла указан идентификатор трафика (в виде наименования pcap-файла), класс устройства и при наличии наименование устройства по следующему формату:

pcap_name	*device_class*	*device_name*
devices1.pcap	1	
devices2.pcap	2	
devices3.pcap	3	
devices4.pcap	5	
….	…	

Одному pcap-файлу соответствует одно устройство.

Классы устройств расшифровываются следующим образом:

1 – Windows;

2 – Android;

3 – IOS;

4 – Телекоммуникационное оборудование;

5 – IoT устройства.

Контрольная выборка Test_1 содержит pcap-файлы с дампом трафика, для которых необходимо определить класс устройства, и, по возможности, наименование устройства, сгенерировавшего данный трафик. Результат необходимо представить в *csv*-файле в формате, указанном в п.3.2. Выборка состоит из 25 файлов.

3.1.2. Исходные данные для задачи выявления сетевых атак

Исходные данные содержат дамп трафика.

Исходные данные разбиты на две выборки: *обучающую и контрольную* (далее Train_2 и Test_2 соответственно).

Обучающая выборка Train_2 включает в себя дамп трафика и экспертную разметку трафика.

Дамп трафика представлен в виде набора pcap-файлов. Для каждого класса атаки предоставляется 50 файлов. Общее количество пакетов в трафике для каждого класса - более 10 000.

Экспертная разметка предоставляется в виде образцов трафика и классов атак и содержится в csv-файле *attacks_train.csv*. В каждой строке файла указан идентификатор трафика (в виде наименования pcap-файла), номера пакетов, идентифицирующих атаку[1], класс атаки и при наличии эксплуатируемая уязвимость по следующему формату:

pcap_name	*packets*	*attack_class*	*vulnerability*
attacks1.pcap	1,3,50,64,189	1	
attacks2.pcap	98,106	2	
attacks3.pcap	137	3	
attacks4.pcap	38,154	4	
….		…	

Одному pcap-файлу соответствует одна атака.

Классы атак расшифровываются следующим образом:

1 – SQL-инъекция;

2 – DOS атака;

3 – эксплуатация уязвимостей посредствам переполнения буфера;

4 – подбор паролей;

5 – XSS-атака.

Контрольная выборка Test_2 содержит файлы с дампом трафика, для которых необходимо определить класс атаки, номера пакетов, указывающих на проведение атаки и, по возможности, наименование эксплуатируемой уязвимости. Результат необходимо представить в *csv*-файле в формате, указанном в п.3.2. Выборка состоит из 25 файлов.

3.2. Формат предоставления результатов

3.2.1. Формат предоставления результатов выполнения задачи идентификации устройств в трафике

Для расчета качества алгоритма идентификации устройств в трафике Участник Конкурса должен предоставить csv-файл, содержащий три столбца:

- столбец наименований файлов с дампом трафика, предоставляемых в контрольной выборке (Test_1);

- столбец классов устройств, являющийся результатом работы алгоритма программы Участника конкурса;

- столбец наименований устройств (при наличии).

pcap_name	*device_class*	*device_name*
devices1.pcap	1	
…	…	…

[1] Номера пакетов указываются перечислением через запятую

3.2.2. Формат предоставления результатов выполнения задачи выявления сетевых атак

Для расчета качества алгоритма выявления сетевых атак Участник Конкурса должен предоставить csv-файл, содержащий четыре столбца:

- столбец наименований файлов с дампом трафика, предоставляемых в контрольной выборке (Test_2);
- столбец номеров пакетов pcap-файла, идентифицирующих ту или иную атаку;
- столбец классов атак, являющийся результатом работы алгоритма программы конкурсанта;
- столбец наименования уязвимости (при наличии).

pcap_name	*packets*	*attack_class*	*vulnerability*
attacks1.pcap	1,3,50,64,189	1	
…		…	

4. Требования к программам

К программам Участников Конкурса предъявляются следующие требования:

а) программа должна реализовывать возможность загрузки множества pcap-файлов, после чего должна выдавать результат в виде csv-файла, содержащего таблицу установленного формата (п. 3.2);

б) программа должна обрабатывать каждый pcap-файл независимо от остальных файлов в выборке (т.е. при обработке не должна использоваться какая-либо дополнительная информация о других файлах);

в) программа должна вести лог решения задачи: в режиме реального времени показывать количество обработанных пакетов, время, затраченное на обработку, и время, необходимое для окончания обработки;

г) программа не должна содержать ошибок исполнения, а также замедлять работу и наносить какой-либо вред вычислительной системе;

д) программа должна предоставляться вместе со всем необходимым для ее запуска программным обеспечением (библиотеки, модули);

е) вся необходимая информация по установке, запуску и функционированию решения должна быть описана в сопутствующей документации;

ж) предоставление необходимых прав на использование программного обеспечения в объемах и сроках, обусловленных воспроизведением результата работы программы, а также помощь в воспроизведении

результатов работы программы является обязанностью Участника Конкурса;

з) время на обработку одного файла размером 5 МБ (не более 5000 пакетов) не должно превышать 30 секунд; данные ограничения приведены в предположении запуска программы на ПК с характеристиками Intel Core i5 - 2500К 3.3 - 3.7 ГГц, 8 Гб ОЗУ или аналогичными;

и) Программа должна запускаться и функционировать на операционных системах Linux: Ubuntu 18.04, CentOS 7, Debian 9;

к) Решения, не удовлетворяющие перечисленным требованиям, к оценке не допускаются.

5. Построение предварительного рейтинга

Критериями построения предварительного рейтинга Участников Конкурса являются:

а) наличие лога решения задачи: в режиме реального времени необходимо показывать:

- количество обработанных файлов;
- время, затраченное на обработку этих файлов;
- наименование текущего обрабатываемого файла;

б) полнота документации: предоставляемая документация должна содержать следующие разделы:

- инструкция по установке программы;
- инструкция по запуску программы;
- описание программы;

в) время обработки файла: тестирование времени обработки будет производиться для файла размером 5 МБ (не более 5000 пакетов) на ПК с характеристиками, аналогичными Intel Core i5 - 2500К 3.3 - 3.7 ГГц, 8 Гб ОЗУ.

За выполнение каждого критерия начисляются баллы в соответствии со следующей таблицей:

Критерий		Количество начисляемых баллов
Наличие лога решения		1,5
Полная документация		1
Время обработки (для файла размером 5 МБ)	0-5 секунд	3
	6-15 секунд	2
	15-30 секунд	1

В соответствии с выставленными баллами строится предварительная рейтинговая таблица Участников конкурса.

6. Оценка качества

6.1. Оценка качества результатов выполнения задачи идентификации устройств в трафике

Расчет качества выполняется на основании результата работы алгоритма Участника, представленного в csv-файле, формат которого описан в п. 3.2.1, а также на основании проверки алгоритма Участника на контрольных примерах Организатора (25 шт.).

Критерием качества решения задачи является количество правильно классифицированных pcap-файлов. При этом за каждый правильно классифицированный pcap-файл начисляется 1 балл.

За каждое верно указанное наименование устройства дополнительно начисляется 1 балл. Также к результату прибавляются баллы предварительной рейтинговой таблицы (п. 5). На основании полученной суммы определяется место Участника в итоговой рейтинговой таблице.

6.2. Оценка качества результатов выполнения задачи выявления сетевых атак

Расчет качества выполняется на основании результата работы алгоритма Участника, представленного в csv-файле, формат которого описан в п. 3.2.2, а также на основании проверки алгоритма Участника на контрольных примерах Организатора (25 шт.).

Для всех pcap-файлов, классифицированных верно, производится оценка качества ответа (насколько корректно алгоритм детектирует признаки атаки в каждом пакете трафика). Для pcap-файла k рассчитываются значения *полноты (recall, r)* и *точности (precision, p)*:

$$r_k = \frac{TP_k}{TP_k + FN_k},$$

$$p_k = \frac{TP_k}{TP_k + FP_k},$$

где *TP (true positive)* — количество пакетов, идентифицирующих атаку и указанных конкурсантом;

FP (false positive) — количество пакетов, не идентифицирующих атаку, но указанных конкурсантом;

FN (false negative) — количество пакетов, идентифицирующих атаку, но не указанных конкурсантом.

На основании полученных значений полноты и точности для pcap-файла k рассчитывается *F-мера:*

$$F_k = 2 * \frac{p_k * r_k}{p_k + r_k}.$$

Для всех pcap-файлов, классифицированных неверно, оценка качества ответа не производится, *F-мера* принимается за 0.

Итоговым критерием качества решения задачи выявления сетевых атак является сумма *F-мер* по всем pcap-файлам. Полученное значение, соответствует количеству начисляемых баллов.

За каждое верно указанное название уязвимости дополнительно начисляется 1 балл. Также к результату прибавляются баллы предварительной рейтинговой таблицы (п. 5). На основании полученной суммы определяется место Участника в итоговой рейтинговой таблице.

6.3. Итоговая оценка результатов

Итоговая оценка результатов по каждой номинации определяется на основании рейтинговой таблицы, полноты представления анкеты проекта, экспертной оценки Конкурсной комиссией доклада Участника Конкурса.