ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

на научно-исследовательскую работу

«Исследование возможности создания автоматизированной системы

выявления скрытых элементов инфраструктуры Tor-сети»

шифр «Наутилус-2»

1. Цель работы состоит в исследовании возможности создания средств автоматизированного идентификации и разбора трафика Tor-сети и составления гипотез об ее инфраструктуре.

2. Обоснование необходимости проведения: в настоящее время отсутствуют успешные реализации средств идентификации трафика Tor-сети и мониторинга скрытых элементов ее инфраструктуры.

3. Основные тактико-технические требования:

* необходимо исследовать существующие методы идентификации сетевого трафика и оценить возможность их применения в каналах передачи данных;
* необходимо разработать методы идентификации трафика Tor-сети и выявления скрытых элементов ее инфраструктуры (внутренние web ресурсы, неопубликованные узлы ит.п.);
* необходимо разработать методы автоматизированного сбора технической информации об объектах инфраструктуры Tor-сети из открытых информационных ресурсов Tor-сети и сети Интернет;
* необходимо разработать методы автоматизированного ведения паспортов объектов инфраструктуры и мониторинга ее изменений;
* необходимо разработать методы автоматизированной классификации материалов, распространяемых с использованием инфраструктуры Tor-сети;
* необходимо создать макет автоматизированной информационной системы, демонстрирующий разработанные научно-технические решения.

4. Предполагаемые результаты: в результате НИР планируется создать макет автоматизированной информационной системы, предназначенной для идентификации трафика Tor-сети и мониторинга скрытых элементов ее инфраструктуры.

5. Сроки проведения:

Начало работы \_\_ квартал \_\_\_\_\_ года

Окончание работы – \_\_ квартал \_\_\_\_\_ года

6. Головной исполнитель: OOО «САЙТЭК» (г. Москва).

7. Стоимость работ: \_\_\_\_\_ тыс. рублей.

КОММЕНТАРИИ

к пояснительной записке на НИР «Наутилус-2»

1. Систематизация программных продуктов, потенциально используемых узлами сетевой инфраструктуры объектов компьютерной разведки, и определение представляющих интерес категорий уязвимостей этих программных продуктов.

Работы по систематизации программных продуктов и уязвимостей направлены на определение иерархий и взаимосвязей продуктов и уязвимостей (в том числе – сведений о видах программных продуктов, их совместимости, версиях, параметрах конфигурации; сведений о видах уязвимостей, условиях их возникновения, влиянии параметров конфигурации и сочетаний программных продуктов), а также ключевых слов, позволяющих связать текстовыесообщения с этими продуктами и уязвимостями.

2. Разработка методов автоматизированного извлечения сведений об уязвимостях программных продуктов из неструктурированной информации, публикуемой на открытых информационных ресурсах.

Автоматизированное извлечение сведений из неструктурированной информации, публикуемой на открытых информационных ресурсах (реплики форумов), должно осуществляться автоматически в соответствии с предусмотренным расписанием специальным программным обеспечением – адаптерами. При сборе информации сохраняются дополнительныеданные (связи между репликами, связи реплик с темами, тэги, сведения об авторах и т.д.). Перечень и параметры доступа к информационным ресурсам определяются экспертом.

3. Разработка методов автоматизированного ведения справочников уязвимостей программных продуктов в соответствии с выбранными категориями.

Предполагается, что информация об уязвимостях программных продуктов, полученная в автоматизированном режиме из неструктурированной информации, публикуемой на открытых информационных ресурсах, включается в справочники уязвимостей после предварительной обработки, которая заключается в унификации (приведении к единой кодировке, языку, формату), классификации (по отношению к программным продуктам и уязвимостям) и оценке значимости (по активности обсуждения и соответствующим ключевым словам). Окончательная оценка собранной информации осуществляется экспертом.

4. Разработка системы признаков технологической информации, свидетельствующих об использовании узлами сетевой инфраструктуры объектов компьютерной разведки определенных программных продуктов (в том числе – признаков конфигураций и версий программных продуктов).

Предполагается, что сведения о программном обеспечении узлов сетевой инфраструктуры содержится в технологической информации, связанной с этими узлами (прежде всего – в исходящем трафике этих узлов). Такие сведения могут быть как достоверными (названия и версии программных продуктов в сообщениях прикладных протоколов, например, сведения о браузере в HTTP-запросах), так и косвенными (особенности текстов сообщений, порядок элементов в сообщении, особенности форматирования, длительность обработки запросов и т.д.).

На основе анализа таких сведений формируется соответствующий набор признаков технологической информации (включая признаки версий и конфигураций программных продуктов).Признакам устанавливаются экспертные оценки достоверности в числовой шкале от 0 до 1 (0 – неинформативный признак; 0,5 – косвенный признак с вероятностью ошибки 0,5; 1 – достоверный признак).

5. Разработка методов автоматизированного определения характеристик программного обеспечения узлов сетевой инфраструктуры объектов компьютерной разведки на основе предложенной системы признаков и методы численной оценки достоверности этих характеристик.

Для автоматизированного определения характеристик программного обеспечения узлов сетевой инфраструктуры предлагается применить механизм автоматической классификации с предварительным обучением. Для обученияклассификатора должен использоваться массив технологической информации, связанный с узлами сетевой инфраструктуры, характеристики программного обеспечения которых заранее известны. В процессе обучения должны выявляться и разрешаться конфликты признаков (ситуации, когда оценки достоверности признаков противоречат друг другу или известным характеристикам программного обеспечения). В рабочем режиме в результате анализа массива технологической информации должныопределяться узлы сетевой инфраструктуры и характеристики их программного обеспечения с соответствующими оценками достоверности этих характеристик.

6. Разработка методов автоматизированного создания паспортов уязвимостей для узлов сетевой инфраструктуры объектов компьютерной разведки на основе определения характеристик программного обеспечения и справочников уязвимостей.

Предполагается, что создание паспортов уязвимостей для узлов сетевой инфраструктуры объектов компьютерной разведки осуществляется в два этапа:

а) автоматическое отнесение полученной информации об уязвимостях к узлам сетевой инфраструктуры объектов компьютерной разведки на основе сведений о характеристиках программного обеспечения этих узлов;

б) этап экспертной обработки, включающий редактирование и пополнение информации об уязвимостях, присвоение маркеров важности, актуальности, применимости, учет результатов использования уязвимостей.