**Сервис управления площадью внешних атак на корпоративную информационную систему
КБ «ЭНЕРГОТРАНСБАНК» (АО)**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

# Общие сведения

## Полное и сокращенное наименования Услуг

Полное наименование: Сервис управления площадью внешних атак на корпоративную информационную систему (КИС).

Сокращенное наименование: «Услуги».

## Плановые сроки оказания Услуг

Окончание оказания Услуг: 1 календарный год с даты заключения договора.

## Цели и задачи Услуг

Целью оказания Услуг является отслеживание актуального состояния внешнего сетевого периметра КИС, определение динамики появления или отсутствия систем, открытых сетевых портов, сетевых служб и их версий, а также своевременное выявление возможных уязвимостей и недостатков, появляющихся на внешнем сетевом периметре в процессе жизненного цикла КИС.

Задачами, решаемыми в ходе оказания Услуг, являются:

* формирование перечня информационных систем (хостов, сетевых сегментов) на внешнем периметре КИС;
* проведение периодического сетевого (инвентаризационного) сканирования;
* проведение периодического сканирования уязвимостей, анализ и актуализация перечня выявленных уязвимостей;
* разработка рекомендаций по устранению выявленных уязвимостей и повышению уровня защищенности.

## Требования к сбору информации об объектах исследования и согласованию исходных данных с Заказчиком

До начала оказания Услуг Исполнителю предоставляется точная информация об объектах исследования:

* список IP-адресов / подсетей целевых систем;
* временные интервалы проведения активных работ.

## Границы оказания Услуг

Объектами исследования в рамках оказания Услуг являются:

* сетевое (инвентаризационное) сканирование:
* не более 256 сетевых узлов (IP-адресов) на внешнем периметре КИС;
* периодичность – 2 раза в месяц;
* сканирование уязвимостей:
* не более 256 сетевых узлов (IP-адресов) на внешнем периметре КИС;
* периодичность сканирования – 1 раз в месяц.

# Состав и содержание Услуг

## Общие требования

Услуги должны оказываться со стороны сети Интернет с IP-адресов, принадлежащих Исполнителю.

Исполнитель должен предпринимать все разумные меры предосторожности, чтобы при оказании Услуг не нарушать нормальную работу компонентов сети Заказчика.

Операции, которые могут привести к деструктивным последствиям (временный отказ в обслуживании), предварительно должны согласовываться с представителями Заказчика и проводиться в специально оговоренное время. Все операции такого рода в обязательном порядке должны протоколироваться. Подобные операции должны проводиться при условии присутствия на рабочем месте ответственного за оказание Услуг со стороны Заказчика.

Если в процессе оказания Услуг возникают сбои оборудования или ПО, Исполнитель должен информировать ответственного со стороны Заказчика об инциденте и оказывать консультативную помощь в его устранении.

## Этапы оказания Услуг

Услуги должны оказываться по следующим этапам:

* сетевое (инвентаризационное) сканирование;
* сканирование уязвимостей;

## Сетевое (инвентаризационное) сканирование

На данном этапе должен проводиться комплекс мероприятий по сетевому сканированию внешнего периметра КИС с целью определения текущего состояния: наличия доступных из сети Интернет сетевых узлов, сетевых портов, сетевых служб и их версий. При оказании услуг должны осуществляться следующие действия:

* инструментальное сетевое сканирование с целью определения доступных сетевых узлов на внешнем периметре КИС;
* инструментальное определение открытых портов, сетевых сервисов, версий прикладного ПО и ОС;
* сравнение полученных результатов с результатами предыдущей итерации, определение изменений в состоянии внешнего периметра КИС;
* формирование результатов итерации сканирования в электронный отчет.

## Сканирование уязвимостей

На данном этапе должен проводиться комплекс мероприятий по выявлению уязвимостей в КИС с помощью специализированных сканеров, а также вручную специалистами Исполнителя. При оказании услуг должны осуществляться следующие действия:

* Проведение автоматизированных проверок специализированными сканерами уязвимостей для оценки состояния защищенности узлов внешнего периметра КИС Заказчика. Сканером выполняются следующие типы проверок:
* определение доступных сетевых узлов посредством TCP и ICMP-сканирования;
* определение открытых портов на доступных сетевых узлах посредством TCP SYN, TCP Full и UDP;
* определение ОС и их версий на основе специфичных для типов ОС ответов серверов;
* выявление криптографических уязвимостей и недостатков SSL/TLS на основе TLS-рукопожатия и SSL-сертификатов серверов;
* выявление уязвимостей и недостатков в версиях сетевых сервисов на основе баннеров (banner grabbing) и сетевых запросов (network probing);
* попытки аутентификации на известных сервисах с применением логинов / паролей по умолчанию;
* выявление известных уязвимостей согласно публичным базам CVE, BID и др.
* Ручной анализ и верификация полученных результатов автоматизированных проверок:
* анализ полученных данных на этапе автоматизированного сканирования;
* выявление ложно-позитивных срабатываний сканера;
* подтверждение выявленных уязвимостей путем ручных проверок узлов и сервисов, на которых были обнаружены уязвимости;
* актуализация перечня выявленных уязвимостей, их категорирование, определение степени критичности.
* Формирование результатов итерации сканирования в виде электронного отчета.

# Требования к результатам оказания Услуг

По результатам сетевого (инвентаризационного) сканирования, в соответствии с установленной периодичностью, Исполнителем должен формироваться и направляться на электронную почту представителей Заказчика электронный отчет-таблица.

Электронный отчет-таблица о сетевом (инвентаризационном) сканировании должен содержать:

* перечень сетевых узлов из сети Интернет;
* перечень открытых сетевых портов;
* перечень сетевых служб и их версий (при возможности), доступных на открытых сетевых портах;
* цветовую подсветку изменений в состоянии внешнего периметра по сравнению с предыдущей итерацией.

По результатам сканирования уязвимостей, в соответствии с установленной периодичностью, Исполнителем должен формироваться и направляться на электронную почту представителей Заказчика электронный отчет-таблица. Исполнитель должен предоставить Заказчику доступ к информационному порталу, содержащему идентичные электронному отчету-таблице сведения о проведенном сканировании уязвимостей.

Электронный отчет-таблица о сканировании уязвимостей должен содержать:

* перечень IP-адресов;
* сетевые имена компьютеров;
* список выявленных уязвимостей, их описание, степень критичности по Common Vulnerability Scoring System (CVSS), общеизвестные идентификаторы (CVE, CWE и др.);
* рекомендации по устранению выявленных уязвимостей.

В конце каждого календарного квартала должен формироваться аналитический электронный отчет. Аналитический электронный отчет должен содержать:

* информацию об общем количестве просканированных сетевых узлов;
* информацию об определенных сетевых портах, сетевых службах и их версиях;
* аналитическую информацию о динамике изменения внешнего сетевого периметра;
* информацию об общем количестве выявленных уязвимостей и недостатков;
* информацию о типах, классах, категориях выявленных уязвимостей;
* графические материалы по динамике выявления и устранения выявляемых уязвимостей;
* перечень наиболее популярных уязвимостей, выявляемых в процессе оказания Услуг;
* аналитическую информацию о динамике изменения внешнего сетевого периметра с точки зрения выявления уязвимостей и недостатков.

# Требования к оформлению результатов оказания Услуг

Результаты оказания Услуг предоставляются в электронном виде – в формате Microsoft Office (DOC, DOCX, XLS, XLSX) или PDF и на информационном портале Исполнителя.