|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.2** | Защита корпоративной почтовой системы от вредоносного программного обеспечения и спама |   **1.1. Описание услуги** | | | | | | |  |
|  | В рамках предоставления услуги для почтовых ящиков в корпоративной почтовой системе, размещенной в центре обработки данных Госкорпорации «Росатом», а также на предприятиях\организациях отрасли.  обеспечивается:  1. Фильтрация нежелательных почтовых сообщений (спама) по типу вложения.  2. Снижение во входящем почтовом трафике спама, вредоносного программного обеспечения, фишинга[[1]](#footnote-1) на базе сигнатурного и эвристического анализа, а также на базе автоматического поведенческого несигнатурного анализа.  Услуга оказывается для почтовых ящиков в корпоративной почтовой системе, размещенной в центре обработки данных Госкорпорации «Росатом», а также на предприятиях\организациях отрасли.  Услуга включает выполнение стандартных запросов, регламентных работ, мониторинг, участие в разборе конфликтных ситуаций и хранение событий информационной безопасности. | | | | | | |  |
|  | **1.2. Способ подключения к ИТ-системе (если необходимо и в зависимости от технической возможности организации)** | | | | | | |  |
|  |  Ярлык на Портале терминальных приложений   Прямая ссылка на Web-ресурс из КСПД   Прямая ссылка на Web-ресурс из интернет (требуется СКЗИ на АРМ / не требуется)   «Толстый клиент» на АРМ пользователя (требуется СКЗИ на АРМ / не требуется)   Другой способ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |  |
|  | **1.3. Группа корпоративных бизнес-процессов / сценариев, поддерживаемых в рамках услуги** | | | | | | |  |
|  | Для данной услуги не применяется | | | | | | |  |
|  | **1.4. Интеграция с корпоративными ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.6. Состав услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Прием, обработка, регистрация и маршрутизация поступающих обращений от пользователей. | | | | |  |
|  | Функциональная поддержка |  | В рамках предоставления услуги Исполнитель осуществляет выполнение следующего перечня основных операций и работ по обслуживанию защиты корпоративной почтовой системы от вредоносного программного обеспечения и спама:   Исполнение политик и стандартов информационной безопасности при выполнении работ по услуге.   Подключение нового почтового домена[[2]](#footnote-2) в рамках объемного показателя, предусмотренного условиями договора.   Фильтрация нежелательных почтовых сообщений по типу вложения.   Создание отчёта о состоянии защиты всего почтового трафика.   Изменение политики защиты почтового трафика в отношении почтового домена.   Участие в разборе конфликтных ситуаций и инцидентов информационной безопасности.   Выработка мер по локализации и предотвращению инцидентов информационной безопасности.   Установление причин неуспешной доставки входящего сообщения.   Анализ и диагностика сбоев или неисправностей, связанных с некорректной работой программного обеспечения.   Устранение сбоев или неисправностей, связанных с некорректной работой программного обеспечения.   Добавление, удаление разграничение прав доступа к программному обеспечению. | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | В рамках предоставления услуги Исполнитель осуществляет выполнение следующего перечня основных операций и работ:   Настройка взаимодействия корпоративной электронной почты на базе MS Exchange с системой защиты от вредоносного программного обеспечения и спама, включая маршрутизацию почтового трафика.   Мониторинг доступности ресурсов программного обеспечения.   Анализ и диагностика сбоев или неисправностей, связанных с некорректной работой программного обеспечения в части ИТ-инфраструктуры.   Устранение сбоев или неисправностей, связанных с некорректной работой программного обеспечения в части ИТ-инфраструктуры.   Поддержка функционирования терминальных сервисов удаленного доступа в объёме достаточном для оказания настоящей услуги (для администрирования самих средств защиты).   Поддержка функционирования службы каталога и встроенных сетевых сервисов в объёме достаточном для оказания настоящей услуги.   Поддержка функционирования серверного оборудования в объёме достаточном для оказания настоящей услуги.   Поддержка функционирования сетевого оборудования в объёме достаточном для оказания настоящей услуги.   Резервное копирование. | | | | |  |
|  | Модификация ИТ-системы |  | Для данной услуги не применяется | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  |  ИТ-система |  |  | | | | |  |
|  |  Портал Госкорпорации «Росатом» |  |  | | | | |  |
|  |  Иное место |  |  | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | Общие ограничения и требования:   Оборудование эксплуатируется в условиях, соответствующих требованиям производителя данного оборудования.   Полный список технологических ограничений (лимитов) определяется при заключении договора.  Специальные требования:   Расчет трудозатрат произведен для 1 (одного) почтового ящика.   В силу технических ограничений программного обеспечения защита почтовых ящиков производиться только в составе всех почтовых ящиков находящихся в почтовом домене. В случае защиты отдельных почтовых ящиков в домене, количество необходимых трудозатрат может быть увеличено на стадии заключения договора.   В зависимости от общего количества почтовых входящих сообщений, вложений и их объема в единицу времени возможна задержка в доставке почтовых сообщений.   Возможны ложные срабатывания, из-за которых письмо может быть не доставлено до получателя.   Исходящие почтовые сообщения и переписка внутри корпоративной почтовой системы не проверяются.   Обновление версий программно-аппаратных комплексов производится в рамках разовых работ по отдельному договору.   Определение возможности резервного копирования определяется исходя из технической возможности при заключении договора.   Максимальное количество обращений пользователей, которые могут быть выполнены без нарушения SLA устанавливается при заключении договора, но не менее 5 % от числа обслуживаемых почтовых ящиков в день.   Период, в течение которого гарантируется поддержка пользователей данной системы: по рабочим дням с 09.00 MSK (UTC+3) до 18.00 MSK (UTC+3). | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  |  Снижение во входящем почтовом трафике вредоносного программного обеспечения, фишинга на базе автоматического поведенческого несигнатурного анализа ("Песочница") - 0,000058567   Снижение во входящем почтовом трафике спама, вредоносного программного обеспечения, фишинга на базе сигнатурного и эвристического анализа. Фильтрация нежелательных почтовых сообщений по типу вложения ("Антиспам") - 0,0000452320 | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | Для данной услуги не применяется | | | | |  |
|  | **1.10. Дополнительные параметры оказания услуги** | | | | | | |  |
|  | 1.10.1. Допустимый простой ИТ-ресурса в течении года, часов |  | 22 | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | 30 | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | 4 | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | 8 | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | Да | | | | |  |
|  | | | | | | | | |

1. Фишинг - вид интернет мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям). Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. [↑](#footnote-ref-1)
2. Только для почтовых ящиков в корпоративной почтовой системе, размещенной в центре обработке данных Госкорпорации «Росатом» [↑](#footnote-ref-2)