|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | СОГЛАСОВАНО:  Главный инженер  \_\_\_\_\_\_\_\_\_ Герасименко О.Н.  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021  Заместитель директора  \_\_\_\_\_\_\_\_\_ Соковикова Н.Б.  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 |  | УТВЕРЖДАЮ:  Начальник УАВИ  ООО «ЭН + Диджитал»  \_\_\_\_\_\_\_\_ Козинцев С.А.    «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2021 |   **Временное техническое решение № ЭН+Д-274 от 03.08.2021**  **Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**  **Срок действия 1.06.2022 года**    **Экземпляр 1, количество листов 11 (включая приложения)** |  |  |

Приложение 5 к Техническому заданию от \_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Предпосылки:** | Актуализация настроек системы электронных очередей «Дамаск» в отделениях ООО «ИЭСБК». Подключение модуля системы электронных очередей «Дамаск» для записи в очередь через сайт ООО «ИЭСБК» - sbyt.irkutskenergo.ru. |
| **Задача:** | Обеспечить безопасное подключение системы электронных очередей «Дамаск» в отделениях ООО «ИЭСБК» в корпоративную информационно вычислительную сеть (КИВС), обеспечив доступ к системе только сотрудникам фронт-офисов ООО «ИЭСБК». Ограничить доступ с серверов системы электронных очередей «Дамаск» к любым ресурсам КИВС, обеспечив передачу информации на выделенный сервер, установленный в серверной исполнительной дирекции по адресу г. Иркутск, ул. Сухэ Батора 3. Обеспечить пользователям, отвечающим за сбор статистики и отчетность, возможность подключения к центральному серверу электронных очередей с минимально необходимыми разрешениями.  Разработать схему безопасного подключения модуля системы электронных очередей «Дамаск» для записи в очередь через сайт ООО «ИЭСБК» - sbyt.irkutskenergo.ru. |
| **Вводное описание:** | Для нужд ООО «ИЭСБК» внедрена система электронных очередей «Дамаск» на филиалах предприятия по Иркутской области. Система включает в себя сервер, табло операторов, аппаратную или программную кнопку вызова клиентов, информационные мониторы, терминалы записи в очередь. Кроме того, для сбора консолидированной информации установлен центральный сервер системы электронных очередей «Дамаск» в серверной по адресу г. Иркутск, ул. Сухэ Батора 3.  Так как система поддерживается сторонней организацией, необходимо ограничить доступ с оборудования системы электронных очередей «Дамаск» в КИВС.  Для работы системы используются следующие порты TCP:  80 – для обмена между серверами электронных очередей  8082 – при использовании аппаратной кнопки вызова клиентов  8083 – при использовании программной кнопки вызова клиентов  8085 – при использовании модуля записи через WEB сайт  445 – для загрузки видеороликов |
| **Ограничения:** | Данное техническое решение является временным и согласовывается на срок до 1 июня 2022 г после прохождения данного срока вносить любые изменения в систему в том числе определенные данным техническим решением - запрещается, за это время должен быть определен владелец системы и подготовлен полный пакет документации на систему включая техническое задание, технический проект, технический паспорт, инструкция пользователя, инструкция администратора. Также в рамках процесса ввода системы в промышленную эксплуатацию подготавливается приказ о вводе системы в промышленную эксплуатацию. Всю организацию работ по документированию и внесению изменений в систему осуществляет владелец системы.  Осуществлять какое-либо дальнейшее развитие системы в рамках данного технического решения - запрещается. |
| **Техническое решение:** | Для реализации данного технического решения необходимо произвести установку оборудования электронных очередей в указанных отделениях ООО «Иркутскэнергосбыт» (Приложение №1) и настроить активное сетевое оборудования корпоративной информационно-вычислительной системы (КИВС) в соответствии данным техническим решением.  Установку оборудования электронных очередей осуществляет подрядная организация в строгом соответствии с данным техническим решением.  Серверы электронных очередей устанавливаются в кроссовых помещениях ООО «Иркутская энергосбытовая компания». Кроссовые помещения закрываются на ключ. Доступ подрядчика в помещения кроссовых осуществляется только в сопровождении сотрудника ООО «ИЭСБК» или специалиста ООО «Эн+ Диджитал».  Для подключения серверов электронных очередей выделяется специально настроенный порт на активном сетевом оборудовании. Оборудование электронных очередей находится в отдельном сегменте сети (Приложение №1), ограниченном списком контроля доступа с минимально необходимыми разрешениями для работы системы. Логическая схема приведена в приложении №3.  Информационные табло, терминалы записи и другое оборудование, необходимое для нормального функционирования системы, находится в сети изолированной от КИВС.  Для возможности записи в электронную очередь через сеть интернет центральный сервер электронных очередей располагается в демилитаризованной зоне на межсетевом экране cisco ASA. Запись в электронную очередь осуществляется с сайта sbyt.irkutskenergo.ru. Обмен между центральным сервером электронных очередей и сайтом осуществляется по протоколу TCP порт 8085.  Предусмотреть возможность доступа к центральному серверу электронных очередей специалистам ООО «ИЭСБК» для формирования отчетов и размещения на центральном сервере электронных очередей видеороликов, для дальнейшей публикации и воспроизведения их на мониторах системы электронных очередей во фронт офисах ООО «ИЭСБК».  Для возможности администрирования серверов электронных очередей подрядчику предоставляется доступ к центральному серверу электронных очередей по протоколу RDP (порт 3389) с использованием сервиса RUSAL Privileged Access Management System (RPAM). Схема доступа к внутренним ресурсам КИВС посредствам RPAM описана в справочном руководстве данной системы. Администрирование удаленных серверов электронной очереди осуществляется по протоколу TCP порт 80.  Все изменения, касающиеся работы системы электронных очередей, в части сопряжения с КИВС, согласуются со специалистами управления по адаптации вычислительной инфраструктуры ООО «ЭН+ Диджитал».  **Настройки активного сетевого оборудования КИВС для функционирования системы электронных очередей:**  Для работы системы электронных очередей в КИВС выбран Vlan id 810, адресация подсетей приведена в приложении № 1.  На маршрутизаторах отделений ООО «ИЭСБК», где будет установлена система электронных очередей, необходимо выполнить следующие настройки:  Вариант 1 с использованием VLAN интерфейсов (cisco800 series, cisco900 series и т.п.)  **router#vlan database**  **router(vlan)#vlan 810 name ElQueue**  **router(vlan)#exit**  **router(config)#interfase vlan111**  **description ### ElQueue ###**  **ip address 172.17.34.XXX 255.255.255.248**  **ip access-group ElQueue\_IN in**  **ip access-group ElQueue\_OUT out**  Вариант 2 с использованием сабинтерфейсов (cisco2900 series, cisco4000 series, и т.п.)  **router(config)# interface GigabitEthernet0/1.810**  **description ### ElQueue ###**  **encapsulation dot1Q 810**  **ip address 172.17.34.XXX 255.255.255.248**  **ip access-group ElQueue\_IN in**  **ip access-group ElQueue\_OUT out**  На коммутаторах отделений, к которым подключается сервер электронной очереди, выполняем следующие настройки:  **switch(config):vlan 810**  **name ElQueue**  **interface fastethernet 0/24**  **switchport mode access**  **switcport access vlan 810**  **description ### ELQueue ###**  Для ограничения доступа из сегмента электронных очередей в КИВС и обратно устанавливаем на интерфейсах списки контроля доступа следующего содержания:  **Extended IP access list ElQueue\_IN**  **10 permit icmp host 172.17.34.XXX any**  **20 permit tcp host 172.17.34.XXX host 10.188.226.100 eq www**  **30 evaluate RL\_ElQueue\_IN**  **40 deny ip any any**  **Extended IP access list ElQueue\_OUT**  **20 permit tcp 172.17.XXX.XXX 0.0.0.XXX host 172.17.34.XXX eq www 8082 8083 reflect RL\_ElQueue\_IN**  **30 permit tcp host 10.188.226.100 host 172.17.34.XXX established**  **40 permit tcp host 10.188.226.100 host 172.17.34.XXX eq www reflect RL\_ElQueue\_IN**  **50 deny ip any any**  где:  **172.17.XXX.XXX 0.0.0.XXX –** подсеть пользователей в отделении ООО «ИЭСБК»  **172.17.34.XXX –** адрес сервера в отделении ООО «ИЭСБК»  **10.188.226.100 –** адрес центрального сервера в ДМЗ.  Добавляем подсети электронных очередей в маршрутизацию на объектах.  **Rouer(config)#router eigrp 1**  **network 172.17.34.XXX 0.0.0.7**    Настройка подключения центрального сервера электронных очередей:  Изменить настройки IP протокола на сетевом интерфейсе сервера  **IP address 10.188.226.100**  **Netmask 255.255.255.0**  **Default gateway 10.188.226.1**  Назначить виртуальной машине использование VLAN id 7 (интерфейс DMZ\_Customers)  На порту коммутатора cisco 6509 (ID-1-C6509) добавить в разрешенные VLAN id 7  **id-1-c6509(config)# interface port-channel 206**  **switchport trunk allowed vlan add 7**  **interface gigabitEthernet 1/1/47**  **switchport trunk allowed vlan add 7**  **interface gigabitEthernet 1/1/48**  **switchport trunk allowed vlan add 7**  **interface gigabitEthernet 2/1/47**  **switchport trunk allowed vlan add 7**  **interface gigabitEthernet 2/1/48**  **switchport trunk allowed vlan add 7**  На межсетевом экране cisco ASA настроить следующие правила для обеспечения работоспособности системы:  Разрешить двухсторонний обмен между центральным сервером электронной очереди (интерфейс DMZ\_Customers) и серверами в отделениях ООО «ИЭСБК» (интерфейс INSIDE). Обмен данными может быть инициирован любой из сторон.  **access-list DMZ\_Customers\_access\_in extended permit tcp object ElQueue\_Server\_IESBK object ElQueue\_Networks\_IESBK eq www**  **access-list inside\_access\_in extended permit tcp object ElQueue\_Networks\_IESBK object ElQueue\_Server\_IESBK eq www**  Разрешить доступ к серверу операторам ООО «ИЭСБК» для возможности создания отчетов и размещения видеороликов для дальнейшей публикации и воспроизведения их на мониторах системы электронных очередей во фронт офисах ООО «ИЭСБК» (интерфейс INSIDE). Для организации доступа к серверу на межсетевом экране создаются две группы:  ElQueue\_operators\_PC80 – группа для специалистов ООО «ИЭСБК» с правом формировать отчетность.  ElQueue\_operators\_PC445 - группа для специалистов ООО «ИЭСБК» с правом размещать видеоролики на общем ресурсе сервера.  Добавление компьютеров пользователей в группы осуществляется по заявкам с обязательным согласованием специалистами УИБ.  **access-list inside\_access\_in extended permit tcp object ElQueue\_operators\_PC80 object ElQueue\_Server\_IESBK eq www**  **access-list inside\_access\_in extended permit tcp object ElQueue\_operators\_PC445 object ElQueue\_Server\_IESBK eq 445**  Разрешить доступ к центральному серверу электронных очередей по протоколу RDP с серверов RPAM для подрядчиков, обслуживающих систему (интерфейс INSIDE):  **access-list inside\_access\_in extended permit tcp object-group RPAM\_Servers object ElQueue\_Server\_IESBK eq 3389**  Разрешить доступ к центральному серверу электронных очередей (интерфейс DMZ\_Customers) с сервера sbyt.irkutskenergo.ru (195.206.48.119) (интерфейс DMZ) по протоколу TCP порт 8085:  **access-list dmz\_access\_in extended permit tcp host 195.206.48.119 object ElQueue\_Server\_IESBK eq 8085**    Network Objects  **ElQueue\_Server\_IESBK – 10.188.226.100**  **ElQueue\_operators\_PC80 – компьютеры пользователей с правом формировать отчеты.**  **ElQueue\_operators\_PC445 - компьютеры пользователей с правом размещать видеоролики.**  **ElQueue\_Networks\_IESBK – 172.17.34.0 255.255.255.0**  **RPAM\_Servers1 – 172.16.48.163**  **RPAM\_Servers2 – 172.16.48.195**  Network Objects Group  **RPAM\_Servers – RPAM\_Server1, RPAM\_Serbver2** |
|  |  |

|  |  |
| --- | --- |
| **Зоны ответственности:** | За обслуживанием компьютеров пользователей, своевременное обновление ОС и антивирусов на подключаемых объектах, отвечает Управление по установке и тестированию программ для ЭВМ, баз данных ООО “En+ Digital”.  За обслуживание, настройку и мониторинг активного сетевого оборудования, в зоне ответственности группы компаний несет ответственность отдел по адаптации сетевой инфраструктуры для программ ЭВМ, баз данных ООО “ En+Digital”.  За настройку, обслуживание (установка и поддержание в актуальном состоянии операционной системы, установленного ПО, антивирусной программы), мониторинг серверов электронных очередей «Дамаск», отвечает подрядная организация.  Схематично распределение зон ответственности после реализации данного ТР показаны в приложении №2 |
| **Требуемые затраты:** | Рассматриваются индивидуально по каждому новому объекту. |

Приложение №1

**Временное техническое решение № ЭН+Д-274 от 03.08.2021**

**Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**

Адресация

Сети **комплекса электронных очередей «Дамаск»** на объектах.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Адрес** | **Маска подсети** | **Адрес маршрутизатора** | **Адрес сервера** | **Адрес объекта** |
| 10.188.226.0 | 255.255.255.0 | 10.188.226.1 | 10.188.226.100 | г. Иркутск, ул. Сухэ Батора 3 |
| 172.17.34.0 | 255.255.255.248 | 172.17.34.1 | 172.17.34.2 | г. Иркутск, ул. Байкальская, 259 |
| 172.17.34.8 | 255.255.255.248 | 172.17.34.9 | 172.17.34.10 | г. Иркутск, ул. Фридриха Энгельса, 17 |
| 172.17.34.16 | 255.255.255.248 | 172.17.34.17 | 172.17.34.18 | г. Шелехов, 4 м-н, дом 93 А |
| 172.17.34.24 | 255.255.255.248 | 172.17.34.25 | 172.17.34.26 | г. Иркутск, Юрия Тена проезд, 19. |
| 172.17.34.32 | 255.255.255.248 | 172.17.34.33 | 172.17.34.34 | г. Иркутск, ул. Розы Люксембург, 164/1 |
| 172.17.34.40 | 255.255.255.248 | 172.17.34.41 | 172.17.34.42 | г. Слюдянка, ул. Парижской комунны, 7 |
| 172.17.34.48 | 255.255.255.248 | 172.17.34.49 | 172.17.34.50 | г. Шелехов, 3-й квартал, 14 |
| 172.17.34.56 | 255.255.255.248 | 172.17.34.57 | 172.17.34.58 | г. Ангарск, ул. Трудовых Резервов, 34 |
| 172.17.34.64 | 255.255.255.248 | 172.17.34.65 | 172.17.34.66 | г. Ангарск, ул. Мира, 69 (89 кв., 37) |
| 172.17.34.72 | 255.255.255.248 | 172.17.34.73 | 172.17.34.74 | г. Усть-Илимск, ул. Карла Маркса, 35 |
| 172.17.34.80 | 255.255.255.248 | 172.17.34.81 | 172.17.34.82 | г. Усолье-Сибирское, ул. Менделеева, 71 |
| 172.17.34.88 | 255.255.255.248 | 172.17.34.89 | 172.17.34.90 | г. Тулун, пер. Энергетиков, 1 |
| 172.17.34.96 | 255.255.255.248 | 172.17.34.97 | 172.17.34.98 | г. Братск, ул. Ленина, 35 |
| 172.17.34.104 | 255.255.255.248 | 172.17.34.105 | 172.17.34.106 | г. Железногорск, ул. Янгеля, 8 |
| 172.17.34.112 | 255.255.255.248 | 172.17.34.113 | 172.17.34.114 | г. Саянск, микрорайон. Мирный, 30 |
| 172.17.34.120 | 255.255.255.248 | 172.17.34.121 | 172.17.34.122 | г. Нижнеудинск, ул. Октябрьская, д. 1 |
| 172.17.34.128 | 255.255.255.248 | 172.17.34.129 | 172.17.34.131 | г. Черемхово, ул. Ф. Патаки, 4 |
| 172.17.34.136 | 255.255.255.248 | 172.17.34.137 | 172.17.34.138 | г. Братск, ул. Холоднова, 11 |
| 172.17.34.144 | 255.255.255.248 | 172.17.34.145 | 172.17.34.146 | п. Хомутово, ул. Некрасова, 2 |
| 172.17.34.152 | 255.255.255.248 | 172.17.34.153 | 172.17.34.154 | г. Братск, ул. Гайнулина, 1 |
| 172.17.34.160 | 255.255.255.248 | 172.17.34.161 | 172.17.34.162 | г. Усть-Илимск, ул. 50 лет ВЛКСМ, 18 |
| 172.17.34.168 | 255.255.255.248 | 172.17.34.169 | 172.17.34.170 | г. Черемхово, ул. Забойщиков, 26 |

Приложение № 2

**Техническое решение № ЭН+Д-274 от 03.08.2021**

**Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**

Схема подключения.



Приложение №3

**Техническое решение № ЭН+Д-274 от 03.08.2021**

**Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**

Логическая схема.



Приложение №4

**Техническое решение № ЭН+Д-274 от 03.08.2021**

**Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**

Доступ к центральному серверу электронной очереди для формирования отчетов и размещения видеороликов определяется на основании заявок со стороны ООО «ИЭСБК» с обязательным согласованием с управлением по информационной безопасности.

Пользователи с доступом для формирования роликов добавляются в группу «ElQueue\_operators\_PC445 - группа для специалистов ООО «ИЭСБК» с правом размещать видеоролики на общем ресурсе сервера» на сетевом оборудовании

Данной группе разрешается доступ к по порту 445 к серверу в DMZ 10.188.226.100 (PSA-SUO01-B01) на котором размещен файловый ресурс E:\Video\_Otdeleniy\ опубликованный в виде [\\PSA-SUO01-B01\Video\_Otdeleniya$](file:///\\PSA-SUO01-B01\Video_Otdeleniya$)

Для доступа на сервере 10.188.226.100 (PSA-SUO01-B01) создаются локальные учетные записи пользователей. Данным учетным записям дается доступ к сетевой папке [\\PSA-SUO01-B01\Video\_Otdeleniya$](file:///\\PSA-SUO01-B01\Video_Otdeleniya$) с правами на чтение/запись.

Пользователи с доступом для формирования отчетов добавляются в группу «ElQueue\_operators\_PC80 – группа для специалистов ООО «ИЭСБК»» на сетевом оборудовании.

Для разграничения доступа для каждого пользователя на центральном сервере 10.188.226.100 (PSA-SUO01-B01) заводятся отдельные учетные записи с правами доступа только к данным своего отделения.

Права доступа в системе определяются согласно матрице ролей, согласованной отдельно.

Администрирование сервера и контроль учетных записей осуществляет подрядная организация.

**Врменнное техническое решение № ЭН+Д-274 от 03.08.2021**

**Организация подключения комплекса электронных очередей «Дамаск» в КИВС в отделениях ООО «Иркутская Энергосбытовая Компания» с возможностью записи в очередь через WEB сайт компании (sbyt.irkutskenergo.ru).**

**Лист согласования.**

**Подписи. ООО «Эн+ Диджитал»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п./п** | **Ф.И.О.** | **Должность** | **Дата** | **Подпись** | **Примечание** |
| 1 | Урбанович Ю.В. | Начальник ОАСетИ |  |  |  |
| 2 | Макаревич И.Г. | Начальник ОАСИ |  |  |  |
| 2 | Борисов М.П. | Главный специалист |  |  | разработчик |

**Подписи. ООО «Иркутскэнергосбыт»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Ф.И.О.** | **Должность** | **Дата** | **Подпись** | **Примечание** |
| 1 | Куц А.В | Начальник отдела ИТ |  |  |  |
| 2 | Мисник А.В. | Ведущий специалист по информационной безопасности |  |  |  |
| 3 | Сугоняко А. А. | Начальник отдела маркетинга |  |  |  |

**Подписи. ООО «ЕвроСибЭнерго-Гидрогенерация»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Ф.И.О.** | **Должность** | **Дата** | **Подпись** | **Примечание** |
| 1 | Скляренок М.В. | Начальник отдела  информационной безопасности УИБ  ДЗР En+ Менеджмент «Сибирь» |  |  |  |