«Астана қаласының Зияткерлік көлік жүйесін кеңейту бойынша жобалау-сметалық
құжаттаманы әзірлеу (құрылыстың 3-ші кезегі)»
жұмыс жобасы бойынша
22.12.2020 ж. № VE-0015/20
(оң)

ҚОРЫТЫНДЫ

ТАПСЫРЫСШЫ:
«Нұр-Сұлтан қаласының көлік және жол-көлік
инфрақұрырылымын дамыту басқармасы» ММ,
Нұр-Сұлтан қаласы

БАС ЖОБАЛАУШЫ:
«Жаңа жобалар ғылыми-техникалық орталығы» ЖШС,
Нұр-Сұлтан қаласы

Нұр-Сұлтан қаласы

АЛҒЫ СӨЗ

«Астана қаласының Зияткерлік көлік жүйесін кеңейту бойынша жобалау-сметалық құжаттаманы әзірлеу (құрылыстың 3-ші кезегі)» жұмыс жобасы бойынша осы жиынтық қорытынды «VIP Expertiza» ЖШС-мен берілді.

«VIP Expertiza» ЖШС-нің рұқсатынсыз осы сараптамалық қорытындыны толық немесе ішінара қайта шығаруға, көбейтуге және таратуға жол берілмейді.

ТОО
VIP
EXPERTIZA

ЗАКЛЮЧЕНИЕ

№ VE-0015/20 от 22.12.2020 г.
(положительное)

по рабочему проекту
«Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)»

ЗАКАЗЧИК:
ГУ «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур-Султан»,
город Нур-Султан

ГЕНПРОЕКТИРОВЩИК:
ТОО «Научно-технический Центр Новые Проекты»,
город Нур-Султан

город Нур-Султан

ПРЕДИСЛОВИЕ

Данное сводное заключение по рабочему проекту «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)» выдано ТОО «VIP Expertiza».

Данное экспертное заключение не может быть полностью или частично воспроизведено, тиражировано и распространено без разрешения ТОО «VIP Expertiza».

НАИМЕНОВАНИЕ: рабочий проект «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)».

Настоящее экспертное заключение выполнено в соответствии с договором №VE/3 от 13 октября 2020 года между ТОО «VIP Expertiza» и ГУ «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур-Султан».

2. ЗАКАЗЧИК: Государственное учреждение «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур-Султан».

3. ГЕНПРОЕКТИРОВЩИК Товарищество с ограниченной ответственностью «Научно-технический Центр Новые Проекты» (государственная лицензия на проектную деятельность от 29.10.2014 года № 14016281, приложение к государственной лицензии от 29.10.2014 года № 001, выданные Комитетом по делам строительства и жилищно-коммунального хозяйства и управления земельными ресурсами. Министерство национальной экономики Республики Казахстан, II категории), г. Астана, субподрядная организация ИП «Табиғат» (государственная лицензия на выполнение работ и оказание услуг в области охраны окружающей среды от 23.05.2016 года № 02395Р, выданная Комитетом экологического регулирования, контроля и государственной инспекции в нефтегазовом комплексе. Министерство энергетики Республики Казахстан).

4. ИСТОЧНИК ФИНАНСИРОВАНИЯ: собственные средства ТОО «Научно-технический Центр Новые Проекты».

5. ОСНОВНЫЕ ИСХОДНЫЕ ДАННЫЕ

5.1 Основание для разработки:

техническое задание от 08.01.2019 года, утвержденное заказчиком;

протокол совещания от 05.04.2018 года № 18-01-7.2, утвержденный Акимом города Астаны;

адресная программа светофорных объектов от 2018 года, утвержденная заказчиком;

протокол технического совещания по вопросам выбора поставщиков материалов от 05.11.2020 года;

топографическая съемка М 1:500, выполненная ТОО «Астанагорархитектура» (государственная лицензия ГСЛ № 002108 от 30.11.2000 года, Агентство Республики Казахстан по делам строительства и жилищно-коммунального хозяйства), ТОО «Гео Изыскания» (государственная лицензия № 14014170 от 24.09.2014 года, Комитет по делам строительства и жилищно-коммунального хозяйства Министерства регионального развития Республики Казахстан. Министерство регионального развития Республики Казахстан)

отчет по инженерно-геологическим работам от 2018 года, выполненный ТОО «Гео Строй Центр» (государственная лицензия № 15011364, приложение к лицензии № 001 от 16.06.2015 года, выданная ГУ «Управление государственного архитектурно-строительного контроля города Астаны» Акимат города Астаны), ТОО «Инженерный центр «Астана» (государственная лицензия № 002587 от 09.01.2001 года, выданная Агентством

Республики Казахстан по делам строительства и жилищно-коммунального хозяйства, г. Астана)

Письма:

письмо на проведение вневедомственной экспертизы от 04.11.2020 года № 503-10-09/1302;

письмо ГУ «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нұр-Сұлтан» об отсутствии необходимости архитектурно-планировочного задания, актов отвода земли от 04.04.2019 № 503-10-09/801;

письмо о сроках продолжительности строительства объектов от 25.12.2019 года №503-10-09/2167;

письмо о реализации Договора от 10.10.2019 года № 503-10-09/1813;

письмо-согласие ТОО «НТЦ НП» на финансирование экспертных услуг от 09.10.2020 года № 10/175;

письмо ГУ «Управления транспорта и развития дорожно-транспортной инфраструктуры г. Нур-Султан» о финансировании работ по проведению экспертизы ТОО «НТЦ НП» от 09.10.2020 года № 503-10-09/1159;

письмо ГУ «Управления транспорта и развития дорожно-транспортной инфраструктуры г. Нур-Султан» по определению затрат от 04.12.2020 года № 503-10-09/1529;

отказное письмо Департамента Комитета технического регулирования и метрологии по городу Астане о процедуре обязательного подтверждения соответствия от 08.08.2017 года № 26-7-11-1-30/931;

отказное письмо Департамента Комитета технического регулирования и метрологии по городу Астане о процедуре обязательного подтверждения соответствия от 12.06.2017 года № 26-7-11-1-30/648.

Технические условия:

АО «Трансгелеком» от 16.05.2019 года № 588/АСТ-И на прокладку кабеля;

Письмо АО «Трансгелеком» от 09.10.2020 ТТС/1255/ФСЕ-И о продлении технических условий от 16.05.2019 года № 588/АСТ-И;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 614 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 615 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 616 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 617 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 618 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 619 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 620 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 621 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО

«Казахтелеком» от 06.11.2020 года № 622 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 623 на прокладку кабеля;

Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2 Центральная региональная дирекция телекоммуникаций – Филиал АО «Казахтелеком» от 06.11.2020 года № 625 на прокладку кабеля;020 года № 624 на прокладку кабеля;

АО «Астана – Региональная Электросетевая Компания» от 05.09.2019 года № 5-Б-182-1601 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 06.03.2019 года № 5-Б-182-361 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 05.09.2019 года № 5-Е-182-1597 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 17.09.2019 года № 5-А-182-1702 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 18.09.2019 года № 5-Б-182-1711 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 19.09.2019 года № 5-Е-182-1728 на проектирование и присоединение к электрическим сетям;

АО «Астана – Региональная Электросетевая Компания» от 19.06.2019 года № 5-С-182-1032 на проектирование и присоединение к электрическим сетям.

Письмо АО «Астана – Региональная Электросетевая Компания» от 05.09.2019 года № 5-Е-182-1599 о внесении изменений в технические условия;

Письмо АО «Астана – Региональная Электросетевая Компания» от 04.03.2019 года № 5-А-182-331 о внесении изменений в технические условия;

АО «Астана – Региональная Электросетевая Компания» от 07.02.2019 года № 5-А-182-197 на проектирование и присоединение к электрическим сетям.

5.2 Согласования заинтересованных организаций:

ГУ «Управление охраны окружающей среды и природопользования города Нур-Султан» Акимата города Нур-Султан» - разрешение на эмиссии в окружающую среду для объектов IV категории № KZ32VDD00156748 от 21.12.2020 года.

5.3 Перечень документации, представленной на экспертизу

ТОМ 1 Общая часть.

ТОМ 2 Автоматизированные системы управления дорожным движением (АСУДД).

ТОМ 3 Наружные сети связи (НСС)

ТОМ 4 Архитектурно-строительные решения (АС).

ТОМ 5 Оценка воздействия на окружающую среду.

ТОМ 6 Локально-сметный расчет.

5.4 Цель и назначение объекта строительства

Оптимизации системы управления улично-дорожной сети города Нур-Султан путем внедрения новых светофорных объектов на наиболее значимых участках улично-дорожной сети города в целях повышения пропускной способности автомагистралей, снижения задержек в движении транспорта, улучшения условий безопасности дорожного

движения, сокращения средней продолжительности поездки, минимизации затрат горючего, снижение выбросов вредных веществ.

Создание систем и/или средств автоматизации технологических процессов на основе программно-технических комплексов.

6. ОСНОВНЫЕ ДАННЫЕ ОБЪЕКТА И ПРИНЯТЫЕ ПРОЕКТНЫЕ РЕШЕНИЯ

6.1 Место размещения объекта и характеристика участка строительства:

Территория строительства расположена в городе Нур-Султан.

Природно-климатические условия участка строительства:

климатический район (СН РК 2.04-01-2017)	- IВ;
дорожно-климатическая зона	- IV;
нормативный вес снегового покрова (III снеговой район)	- 100 кгс/кв.м;
нормативный скоростной напор ветра (III снеговой район)	- 38 кгс/кв.м;
расчетная зимняя температура наружного воздуха наиболее холодной пятидневки (СН РК 2.04-01-2017)	- минус 31,2°С;
нормативная глубина промерзания грунтов:	
суглинки и глины	- 171 см;
супесь, пески мелкие и пылеватые	- 208 см;
пески средние, крупные и гравелистые	- 222 см;
крупнообломочные грунты	- 253 см.

район не сейсмоактивен (СН РК 2.04-01-2017)

Инженерно-геологические условия площадки строительства

Согласно технического отчета по инженерно-геологическим изысканиям, выполненный ТОО «Гео Строй Центр» от 2019 году в геоморфологическом отношении участок проектирования приурочен к границе правобережной надпойменной террасы р. Ишим и гряды Казахского мелкосопочника вытянутой с юго-запада на северо-восток. Поверхность участка непосредственногопроектирования и прилегающей территории носит характер слабонаклонной равнины, уклонповерхности в западном направлении. Абсолютные отметки участка проектирования в пределах 368,89 – 369,16м (по устьям скважин).

В геологическом строении участка принимают участие породы мезо-кайнозойской коры

выветривания кремниевых сланцев (eMz) представленные суглинками, с прослоями

останцев материнских пород.

В геологическом строении района проектирования участка, на исследованную глубину

4,0м, принимают участие пролювиально-делювиальные отложения средне –

верхнечетвертичного возраста (pdQII-III) представленные суглинками и глинами полутвердой

консистенции с прослоями песка насыщенного водой.

Современные образования представлены конструктивными слоями дорожной одежды

состоящая из асфальтобетонного покрытия, щебёночной смеси метаморфических пород с

суглинистым заполнителем и насыпным грунтом представленный суглинком с дресвой

слежавшийся более 5 лет.

Подземные воды на участке проектирования скважинами глубиной 4,0 м не вскрыты

Современные образования (tQIV).

ИГЭ 0 – существующая дорожная одежда представленная двумя конструктивными

слоями: покрытие – горячий асфальтобетон h=9÷10см; основание – щебеночная смесь

метаморфических пород h=16÷19см. Мощность слоя от 0,25.0,29 м.

ИГЭ 1 – насыпной грунт - суглинок серо-желто-коричневого цвета, твердой консистенции,

использовался при планировочных работах для доведения до проектной отметки, вскрыт

повсеместно под дорожной одеждой. Мощность слоя 3,35.3,11м.

Элювиальные мезозойские образования (eMz).

ИГЭ 2 – суглинок серо-розового цвета, твердой консистенции, с незначительными

включениями дресвы. Мощность слоя скважинами глубиной 4,0 м не определена. Вскрытая

мощность слоя составила 0,4 - 0,6 м.

Грунты слагающие верхний горизонт исследуемого участка повсеместно подвержены морозному пучению.

Физико-механические свойства приводятся в таблице:

№№ п/п	Наименование Характеристики	Обозначение	Единица Измерения	ИГЭ-2
1	Плотность грунта в условиях естественного залегания	ρII ρI	г/см3 г/см3	2.04 2.01
2	Удельное сцепление	CII CI	кПа кПа	51 34
3	Угол внутреннего трения	φII φI	град град	21 18
4	Модуль деформации	E	МПа	15
5	Условное расчетное сопротивление	R○	кПа	263

Согласно лабораторных данных грунты слагающие участок проектирования

незасоленные (ГОСТ 25100), обладают слабой сульфатной агрессией к бетонам марки W4 – W8 на портландцементе, а так же слабой хлоридной агрессией к железобетонным конструкциям. Коррозийная активность грунтов по отношению к углеродистой стали от средней до высокой.

6.2 Проектные решения

6.2.1 Общестроительные работы

Общестроительными работами предусмотрено:

установка светофорных конструкций и шкафов (контролера и ИБП) на 65 реконструируемых объектах;

установка 110 информационных табло на остановочных пунктах;

установка опор детектирования транспортных потоков на 118 объектах;

установка опор видеонаблюдения транспортных потоков на 30 объектах;

установка VMS табло на конструкцию ИЩДУ-8000 для комплекта метеостанций;

установка магистральных шкафов связей на четырех объектах проекта;

установка контейнера ЦОД;

прокладка коммуникаций в траншее типа Т-2.

6.2.2 Конструктивные решения

Уровень ответственности сооружения - II.

Степень огнестойкости сооружения - II.

Класс функциональной пожарной опасности - Ф5.3

Класс конструктивной пожарной опасности сооружения – С3.

Расчет фундаментов сооружений выполнен ТОО «НТЦ НП» на основные сочетания нагрузок. Конечным результатом является определение размеров фундаментов.

Конструкции и материалы приняты следующие:

фундаменты – под стойки пешеходные, транспортные и стойки кнопки ТВП столбчатые с размерами 800х800х1000(h) мм. Выполнены из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается стакан для стоек из трубы диаметром 159х4 мм по ГОСТ10704-91, высотой 1000 мм. Фундаменты армируются арматурой диаметром 10А400 по ГОСТ 34028-2016. Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундаменты – под консоли светофорные и опоры Stick столбчатые с размерами 1000х1000х2000(h) мм. Выполнены из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается стакан для стоек из трубы диаметром 219х6 мм по ГОСТ10704-91, высотой 2000 мм. Фундаменты армируются арматурой диаметром 10А400 по ГОСТ 34028-2016.Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундаменты – под опоры Stick столбчатые с размерами 1000х1000х2000(h) мм. Выполнены из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается стакан для стоек из трубы диаметром 159х4 мм по ГОСТ10704-91, высотой 2000 мм. Фундаменты армируются арматурой диаметром 10А400 по ГОСТ 34028-2016.Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундаменты – под опоры молниеотвода столбчатые с размерами 1000х1000х1200(h) мм. Выполнены из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается стакан для стоек из трубы по ГОСТ10704-91, высотой 1200 мм. Фундаменты армируются арматурой диаметром 10А400 по ГОСТ 34028-2016.Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундаменты – под опоры SAL и СТ-16 столбчатые с размерами 1000х1000х2000(h) мм. Выполнены из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается стакан для стоек из

трубы диаметром 275х5 мм по ГОСТ10704-91, высотой 2000 мм. Фундаменты армируются арматурой диаметром 10А400 по ГОСТ 34028-2016.Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундамент – под магистральный шкаф столбчатый с размерами 1000х1000х1000(h) мм. Выполнен из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается полиэтиленовые трубы диаметром 110 мм. В тело фундамента устанавливается пространственная рама из равнополочных уголков 50х по ГОСТ 8509-93. Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундамент – под шкаф АСУДД, ИБП столбчатый с размерами 800х800х550(h) мм. Выполнен из бетона класса по прочности В30, класса по водонепроницаемости W10, Класса по морозостойкости F10. В тело фундамента устанавливается пространственная рама из равнополочных уголков 50х по ГОСТ 8509-93. Под фундаментами предусмотрена щебеночная подготовка толщиной 100 мм;

фундамент – ФМС1 под опору ИЩДУ-8000 с размерами по подошве 2100х2100х900(h) мм, высотой 2100 мм. Выполнен из бетона класса по прочности В25. Подошва фундамента армируется сеткой из арматуры диаметром 16А400 по ГОСТ 34028-2016 с шагом 200х200 мм. Стакан армируется пространственным каркасом с вертикальной арматурой диаметром 16А400 по ГОСТ 34028-2016 и горизонтальной арматурой диаметром 10А240 по ГОСТ 34028-2016 с шагом 200 мм;

гидроизоляция – выполнена обмазкой битумным праймером за два раза;

стойки - пешеходного светофора марки Sal SYG алюминиевая, высотой 4,0 м. Транспортного светофора марки Sal SYG алюминиевая, высотой 5,0 м. Установка на фундамент выполняется болтами класса точности В марки М16 по ГОСТ 7798-70;

консоль - пешеходного светофора марки Sal SYG алюминиевая, длиной 7,0 м. Установка на фундамент выполняется болтами класса точности В марки М27 по ГОСТ 7798-70;

стойки - опоры марки Stick алюминиевая, высотой 3,0 м. Установка на фундамент выполняется болтами класса точности В марки М20 по ГОСТ 7798-70;

стойки - опоры молниеотвода марки НФГ-5,0-3(2) –ц алюминиевая, высотой 7,0 м. Установка на фундамент выполняется болтами класса точности В марки М16 по ГОСТ 7798-70;

стойки - опоры марки СТ-16 из оцинкованной стали, высотой 16,0 м. Установка на фундамент выполняется болтами класса точности В марки М24 по ГОСТ 7798-70;

стойки - опоры стойки ТВП высотой 3,0 м. Установка на фундамент выполняется болтами класса точности В марки М16 по ГОСТ 7798-70;

кронштейн – для видеокамеры выполнен из прямоугольной трубы 40х25х3 по ГОСТ 8645-68, длиной 1200 мм. Подкос кронштейна выполнен из трубы диаметром 15х2.8 по ГОСТ 3262-75, длиной 1200 мм. Кронштейн разработан для подвижной видеокамеры на опору СТ-16;

опора – для крепления светофорного оборудования выполнено из прямоугольной трубы 40х25х1.5 по ГОСТ 8645-68, длиной 1170 мм. После изготовления на изделие наносится цинковое покрытие;

опора – для крепления пешеходного светофорного оборудования выполнено из прямоугольной трубы 40х25х1.5 по ГОСТ 8645-68, длиной 620 мм. После изготовления на изделие наносится цинковое покрытие;

опора – для крепления пешеходного таймера выполнено из прямоугольной трубы 40х25х1.5 по ГОСТ 8645-68, длиной 520 мм. После изготовления на изделие наносится цинковое покрытие;

опора – ИЩДУ-8000 состоит из стойки и рамы. Стойка выполнена из квадратной трубы 200х6 по ГОСТ 8645-68, высотой 8000 мм. Рама выполнена из квадратной трубы 100х5 по ГОСТ 8645-68. После изготовления на изделие наносится цинковое покрытие;

ограждение – резервной серверной ЦУТ состоит из столбов, панелей, ворот и калитки. Столбы выполнены из прямоугольных (60х40х1.5 мм) и квадратных (100х3, 60х2 мм) по ГОСТ Р 57278-2016, высотой 2,5 и 2,7 м. Панель типа Оригинал, ворота и калитка по ГОСТ Р 57278-2016.

Мероприятия по защите конструкции

Защита конструкций от коррозии предусмотрена в соответствии с требованиями

СП РК 2.01-101-2013 «Защита строительных конструкций от коррозии».

Боковые поверхности бетонных и железобетонных конструкций, соприкасающиеся с грунтом, выполняется обмазкой битумным праймером за два раза.

Металлические элементы окрашиваются лаком БТ-577 и краской БТ-177 по ГОСТ 5631-79 за два раза.

После изготовления на некоторые изделие наносится цинковое покрытие;

Противопожарные мероприятия выполнены в соответствии с СП РК 2.02-101-2014 «Пожарная безопасность зданий и сооружений».

6.2.5 Инженерное обеспечение, сети и системы

Наружные сети связи

Проект разработан на основании архитектурно-строительных, сантехнических заданий и в соответствии с нормативными документами:

Задание на проектирование, выданное заказчиком.

РД 50-34.698-90. Автоматизированные системы требования к содержанию документов;

РД 78.36.002-99. Технические средства систем безопасности объектов. Обозначение условно графические элементов системы;

ВСН 116-93. Инструкция по проектированию линейно-кабельных сооружений связи;

РДС РК 4.04-191-2002. Методические указания по проектированию городских и поселковых электрических сетей;

ГОСТ 23545-79. Автоматизированные системы управления дорожным движением. Условные обозначения на схемах и планах;

ГОСТ 23457-86. Технические требования организации дорожного движения. Правила применения;

Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;

Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года №832;

СТ РК ИСО/МЭК 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования»;

СТ РК ИСО/МЭК 27002-2015 «Информационная технология Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации»;

СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты» Свод правил по управлению защитой информации»;

СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

СТ РК 1125-2002. Знаки дорожные. Основные технические условия;

СТ РК 1124-2003. Технические средства дорожного движения. Разметка дорожная. Технические требования;

СТ РК 1378-2005. Дороги автомобильные. Учет интенсивности движения.

СНиП РК 4.04-07-2013 "Электротехнические устройства"

ПУЭ РК 2015г. Правила устройства электроустановок.

СНиП РК 1.02-03-2011 «Порядок разработки, согласования, утверждения и состав проектной документации на строительство»

СП РК 4.04-101-2013 «Проектирование городских и поселковых электрических сетей»

Шифр А-2011 «Прокладка кабелей напряжением до 35кВ в траншеях. Выпуск 1. Материалы для проектирования и рабочие чертежи».

Проектные решения.

Общие данные

В данной пояснительной записке представлена информация по разработке комплекса мер для обеспечения информационной безопасности объекта инфраструктуры ТОО "Астана LRT".

В рамках проектирования была проведена предварительная оценка состояния защищенности ИТ инфраструктуры предприятия сети ИТС в которой размещено оборудование программно-аппаратных комплексов, обеспечивающих функционирование ITS и других систем, эксплуатируемых компанией АЛРТ.

По результатам предварительной оценки состояния информационно-телекоммуникационной инфраструктуры сети ИТС выявлены две наиболее критичные в плане рисков информационной безопасности системы:

Электронная система оплаты проезда – в случае получения несанкционированного доступа к данной системе злоумышленник получит возможность осуществить как деструктивные действия, которые могут повлечь за собой негативные последствия вплоть до приостановки работы системы и необходимости проведения восстановительных процедур, так и действия мошеннического характера;

Система адаптивного управления дорожным движением - в случае получения несанкционированного доступа злоумышленник сможет дезорганизовать работу светофорных объектов, тем самым создать хаос на дорогах города, который может привести к непредсказуемым последствиям.

В случае реализации вышеперечисленных рисков предприятие понесет финансовые и репутационные потери.

По результатам предварительной оценки на соответствие требованиям нормативной документации (Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности и т.д.)

условий размещения серверного и телекоммуникационного оборудования ИТС, можно констатировать, что имеются следующие основные недостатки, которые могут негативно повлиять на бесперебойное функционирование и состояние информационной безопасности:

- Отсутствует система резервирования (зеркалирования) серверов по типу N+1;
- Помещение серверной не оснащено системой автоматического газового пожаротушения;
- Отсутствует система контроля и управления доступом в серверной комнате (СКУД);
- Микроклимат (температура, влажность) в серверном помещении нарушен – отсутствует система прецизионного кондиционирования;
- В серверном помещении не реализованы мероприятия по защите от утечки информации по каналам побочных электромагнитных излучений и наводок;
- Отсутствует система охранного видеонаблюдения в серверном помещении;
- В помещении серверной имеются незащищенные окна с выходом на открытое уличное пространство.

Компоненты, географически распределенной по территории города, сетевой инфраструктуры не защищены системой охранной сигнализации в местах их установки.

С учетом имеющегося опыта и анализа лучших мировых практик в сфере обеспечения бесперебойного функционирования и информационной безопасности критических информационных систем, а также учитывая перенос основных информационных систем в сторонний ЦОД организовали резервный ЦОД на базе контейнера. Данный подход обеспечивает мобильность и масштабируемость резервного ЦОД, повышает его надежность за счет применяемых технических решений и полномасштабного, комплексного тестирования всех подсистем ЦОД производителем.

Для обеспечения физической сохранности и предотвращения несанкционированного доступа к телекоммуникационному оборудованию, являющегося основой транспортной среды ИТС использовали систему мониторинга физического доступа с возможностью развертывания системы контроля на базе пульта централизованного наблюдения с реагированием мобильных групп подрядной охранной организацией.

В этой связи, для приведения состояния системы защиты информации предприятия в соответствие с Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности (ПП №832 от 20 декабря 2016 года), стандартов в сфере ИБ 27001, 27002 и т.д., а также принимая во внимание серьезность и высокую вероятность реализации вышеприведенных рисков предусмотрено построение системы защиты информации в сети ИТС, для этого внедрили следующие системы обеспечения безопасности информации:

- Предусмотрели разработку и внедрение нормативной документации согласно требованиям стандартов РК;
- Программный продукт по проверке соответствия нормативным требованиям;
- Программно-аппаратный комплекс контроля доступа к сети ИТС;
- Программно-аппаратный комплекс NGFW Cisco 2110;
- Программный продукт Cisco StealthWatch;
- Межсетевой экран Cisco ASA5525 FirePower;

– Программный продукт для контроля за действиями привилегированных пользователей в сети;

– Маршрутизатор CISCO ASR1001-X.

– ЦОД контейнерного типа;

– Система мониторинга физического доступа.

Инфраструктура сети ИТС представлена на схеме:

- Сеть передачи данных ИТС;
- Технологические решения
- Сеть передачи данных ИТС
- По результатам проведенного обследования сети передачи данных ИТС, на объекте установлены:
- Программный продукт FortiClient;
- Cisco FW ASA 5525
- Исходя из анализа возможных угроз информационной безопасности, определены следующие компоненты для внедрения в сеть передачи данных:
- Программный продукт MaxPatrol 8
- Нормативное регулирование
- Программно-аппаратный комплекс NGFW Cisco 2110;
- Программный продукт Cisco StealthWatch;
- Межсетевой экран Cisco ASA5525 FirePower.
- Программный продукт Cisco ISE;
- Программный продукт Indeed PAM;
- Маршрутизатор CISCO ASR1001-X.

Описание программного обеспечения и технические характеристики оборудования:

- Сеть предприятия ИТС.
- Программный продукт MaxPatrol 8
- Контроль защищенности и соответствие стандартам (MaxPatrol 8)

MaxPatrol 8 – автоматизированное решение, позволяющее оценивать уровень защищенности информационных ресурсов всей организации. MaxPatrol автоматизирует процесс поиска уязвимостей и контроля соответствия техническим стандартам в IT-инфраструктуре любого масштаба.

MaxPatrol объединяет все необходимые механизмы оценки уровня безопасности:

- тестирование на проникновение (PenTest) – анализ защищенности со стороны внешнего нарушителя, не имеющего сведений о системах;
- системные проверки (Audit) – контроль уязвимости программного обеспечения и настроек систем в сети организации;
- контроль соответствия стандартам (Compliance) – анализ соответствия систем отраслевым или внутренним стандартам, а также проверка соответствия настроек лучшим мировым практиками.

MaxPatrol позволяет контролировать параметры более 1000 платформ и приложений сетевую и системную инфраструктуры, серверы, беспроводные сети и сети IP-телефонии, базы данных, приложения, системы ERP и веб-приложения.

При этом MaxPatrol решает задачи безопасности информационных систем на всех структурных уровнях организации: от специалистов IT-отделов до первых лиц компании. Автоматизация всех процессов в системе MaxPatrol, от сканирования до формирования отчетов, даст возможность повысить точность получаемой информации, экономить ресурсы и выстроить процесс управления уязвимостями.

MaxPatrol 8 — система оценки защищенности, выполняет сканирование в режиме Аудит (проверку на уязвимости конфигурации систем и на наличие уязвимостей), проверку на соответствие стандартам (Compliance) и тестирование на проникновение методом черного ящика, а также выпускает отчеты различного типа по результатам сканирования. Продукт может использоваться для проверки на соответствие стандарту PCI DSS, ISO, GDPR.

MaxPatrol позволяет проводить тестирование на проникновение, оценку приложений, инвентаризацию сетей и проверку сетевого периметра.

Межплатформенная совместимость:

- сетевое оборудование Cisco, Juniper, Check Point, Arbor, Huawei, Nortel, Alcatel и др.;
- беспроводные VOIP-устройства и телекоммуникационное оборудование;
- операционные системы Windows, Linux, IBMAIX, HP-UX и Oracle Solaris;
- базы данных, включая Microsoft SQL, Oracle, IBMDB2, PostgreSQL, MySQL, Sybase и SAP Hana;
- настольные приложения: веб-браузеры, офисные приложения, службы мгновенных сообщений;
- инфраструктурные приложения, включая Active Directory, Microsoft Exchange, IBM Lotus, Microsoft IIS, Apache, IBM WebSphere, Apache Tomcat;
- платформы терминалов и виртуализации: VMware vSphere/ESXi, Microsoft Hyper-V, Citrix XenApp и др.;
- системы безопасности: personal IPS, firewalls, антивирусы и др.;
- критически значимые производственные системы: ERP, banking & billing systems, в том числе SAP R/3 и SAP NetWeaver.

Безопасность веб-приложений — оценка веб-приложений, написанных на AJAX, JSON, Flash и Java. Анализ безопасности систем ERP — с использованием различных руководств, таких как SAP Security Guides, ISACA (ITAF).

Аудит политики паролей — проверка методами черного и белого ящика:

- для систем удаленного доступа и VPN (RDP, VNC, Telnet, SSH, RCP и т. п.);
- систем совместного использования файлов и каталогов;
- протоколов приложений: SAP, Oracle, SQL, Web, Email и т. п.;
- настольных приложений, например IM и браузеров.

Обнаружение вредоносного ПО — технология обнаружения небезопасного кода, вредоносного ПО и троянов во всех системах без использования агентов.

Автономная проверка целостности системы — встроенные базы для компонентов каждой системы позволяют обнаружить инциденты или нежелательные изменения.

Гибкая система отчетности — поддерживает автоматизированные процессы, в том числе инвентаризацию, управление изменениями, контроль соответствия стандартам и производительности ИТ.

Интерфейс для интеграции на базе XML — позволяет создать единую инфраструктуру информационной безопасности, реализующую управление ресурсами, связь со службой поддержки, управление рисками, управление исправлениями, SIM/SIEM, IPS- и WAF-тестирование на проникновение, NAC/NAP.

Портал отчетности на базе QlikView — наглядно отображает уровень защищенности по отдельным регионам (например, по субъектам федерации), что особенно полезно при распределенной установке с большим количеством узлов. Это позволяет получить более развернутую и подробную аналитическую картину, дополняя возможности модуля отчетности MaxPatrol

Нормативное регулирование.

Информация – один из самых важных ресурсов любого предприятия. Её своевременное получение, эффективное использование, надлежащее хранение и безопасная передача играют определяющую роль в деятельности предприятия, сказываются на его прибыльности и развитии.

Для работы с информацией использовали самые разнообразные технические устройства (сервера, системы хранения данных, мобильные устройства и т.д.). Чаще всего — это компьютер, как правило в составе корпоративной сети, имеющей подключение к сети Интернет.

Однако есть, конечно, и существенный минус. Информация, хранящаяся в современной информационно телекоммуникационной (далее ИТК) инфраструктуре предприятия и передаваемая по каналам передачи данных, находится под угрозой: её могут уничтожить, украсть, умышленно удалить или исказить. Выход из строя элементов ИТК инфраструктуры также чреват потерей информационных данных. Поэтому они должны быть соответственным образом защищены. Защищены комплексно, от всех возможных рисков.

При разработке системы защиты в основном используется набор технических средств и организационных мер защиты информации.

Основная задача организационных мер — это выработка подхода к корпоративным системам защиты информации.

Область проведения услуг:

- ЦОД, находящийся по адресу (г.Нур-Султан) г. Нур-Султан, ул. Туран 32,
- Серверное помещение, находящееся по адресу г. Нур-Султан, ул. Туран 32,
- Локальные вычислительные сети: ИТС и предприятия АЛРТ.
- Электронные информационные ресурсы.
- Нормативно-техническая и иная документация по управлению информационной безопасности.

Задачи проведения услуг:

- Анализ функций и процессов обеспечения информационной безопасности;
- Анализ организационной структуры информационной безопасности Заказчика;
- Анализ осведомленности сотрудников Заказчика в области информационной безопасности;
- Обследование сети передачи данных;

- Обследование серверного помещения (ЦОД);
- Сканирование на уязвимости;
- Обследование конечных устройств;
- Разработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов управления информационной безопасностью;
- Разработать отчеты по оценке и выработке рекомендаций в разрезе объектов обследования.

Этапы проведения услуг:

Этап 1. Обследование и анализ процессов обеспечения информационной безопасности и организационной структуры.

Обследование и анализ состояния организации работ по выполнению требований согласно пункту 5.1 и внутренним нормативным документам по информационной безопасности с предоставлением Заказчику информации по результатам обследования:

1) положений Политики информационной безопасности;
2) процессов по управлению информационной безопасностью;
3) организации управления активами;
4) обеспечения безопасности, связанной с персоналом;
5) физической защиты оборудования;
6) обеспечения надлежащего и безопасного функционирования средств обработки информации;
7) организации управления доступом к информационным ресурсам;
8) процессов разработки, внедрения и обслуживания информационных систем;
9) организации управления инцидентами в области информационной безопасности;
10) степени соответствия внутренней нормативной документации в области информационной безопасности требованиям действующего законодательства и нормативно-техническим требованиям РК;

Этап 2. Анализ уровня культуры информационной безопасности у сотрудников Заказчика:

1) Проведение обследования с целью сбора доступной информации о Заказчике;
2) Оценка уровня осведомленности сотрудников в области информационной безопасности;

Этап 3. Обследование сети передачи данных

1) Обследование архитектуры построения сети передачи данных;

a. ознакомление с текущей схемой локальной вычислительной сети Заказчика;
b. Обследование логической и физической схем сети Заказчика;

2) Обследование сетевого оборудования: создание списка имеющихся в сети сетевых устройств с серийными номерами и сетевыми адресами;
3) Анализ конфигурационных файлов сетевых устройств: экспорт конфигурационных файлов сетевых устройств и последующий анализ настроек;
4) Выработка рекомендаций по устранению недостатков: включая предложения по дизайну локальной сети с учетом рекомендаций мировых производителей сетевого оборудования.

Этап 4. Обследование серверного помещения (ЦОД)

Обследование серверных помещений на соответствие требованиям пункта 5.1 в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

Этап 5. Сканирование на уязвимости

Инструментальное обследование уязвимостей в сети ИТС средствами специализированного программного-аппаратного комплекса по выявлению уязвимостей информационной безопасности с выдачей рекомендации по их устранению.

Этап 6. Обследование конечных устройств

1) Обследование на соответствие аппаратной части выполняемым задачам;
2) Выборочная инвентаризация рабочих станций;
3) Обследование политик безопасности;
4) Сканирование выборочных рабочих станций на наличие уязвимостей.

Этап 7. Разработка методик и внедрение системы управления информационной безопасности:

1) Повышение осведомленности Первого руководителя;
2) Совещание с ключевыми участниками системы информационной безопасности;
3) Формирование/пересмотр целей информационной безопасности;
4) Согласование плана действий по системе управления информационной безопасности;
5) Создание рабочей группы по информационной безопасности;
6) Утверждение структуры документации по информационной безопасности;
7) Утверждение типов активов;
8) Утверждение видов активов;
9) Разработка модели ролей и компетенций системы информационной безопасности;
10) Разработка рекомендаций на создание структурного подразделения;
11) Доработка или разработка политики информационной безопасности;
12) Разработка системы требований (База контролей);
13) Разработка карты рисков;
14) Разработка модели угроз;
15) Определение модели нарушителей;
16) Разработка системы оценки рисков;
17) Оценка рисков;
18) Утверждение стратегии обработки рисков;
19) Разработка правил обращения с активами;
20) Процедура регистрации инцидентов;
21) Процедура управления инцидентами;
22) Журнал регистрации инцидентов;
23) Процедура корректирующих действий;
24) Процедура управления документацией;
25) Процедура оценки эффективности внедрение системы управления информационной безопасности;
26) Операционные процедуры для управления информационными технологиями;
27) Процедура непрерывности бизнеса;
28) Процедуры закупа технических средств;

29) Процедура уведомления сотрудников о внедрении системы управления информационной безопасности;

30) Процедура найма и прекращения найма сотрудников;

31) Процедура проверки знаний правил информационной безопасности;

32) Определение дисциплинарных мер;

33) Политика защиты конечных станций (Endpoint Security);

34) Политика защиты сетевой инфраструктуры (Network Security);

35) Политика защиты почтового трафика (Email Security);

36) Политика управления изменениями (Change Management);

37) Политика управления учётными записями (Identity Management);

38) Политика безопасного хранения данных (Storage Security);

39) Политика управления логами и инцидентами (Incident Management);

40) Политика предотвращения утечки информации (Data Loss Prevention);

41) Политика безопасности корпоративных приложений (Application Security);

42) Политика управления уязвимостями;

43) Политика удаленной работы;

44) Политика контроля доступа;

45) Разработка технической карты физической безопасности в части доступа к помещениям Департамента ИТ, ЦОД, Серверных помещений;

46) Разработка регламента взаимодействия со Службой безопасности;

47) Анализ СУИБ со стороны руководства: определение потребностей в ресурсах.

48) Задачи проведения обследования:

– Идентификация активов, угроз и уязвимостей;

– Оценка уровня защищенности;

– Оценка соответствия требованиям;

– Выработка рекомендаций по повышению уровня защищенности и ликвидации уязвимостей.

Программно-аппаратный комплекс NGFW Cisco2110.

- Устройства Cisco FirePOWER серии 2100

Устройства Cisco Firepower серии 2100 — это семейство из четырех платформ безопасности на базе МСЭ нового поколения с ориентацией на защиту от угроз, обеспечивающих непрерывность бизнеса благодаря непревзойденной защите от угроз. При активации расширенных функций защиты от угроз производительность системы остается стабильной. Эти платформы уникальным образом сочетают в себе инновационную двойную многоядерную архитектуру ЦП, которая оптимизирует одновременную работу функций МСЭ, шифрования и обнаружения угроз. Пропускная способность устройств находится в диапазоне от 1,9 до 8,5 Гбит/с, что позволяет использовать их в самых разных вариантах развертывания - от периметра Интернета до ЦОД.

- Поддерживаемые платформы

Межсетевой экран нового поколения Cisco Firepower включает следующие функции: мониторинг и контроль приложений (AVC), дополнительная система защиты от вторжений нового поколения Firepower next-gen IPS (NGIPS), защита от усовершенствованного вредоносного ПО Cisco® Advanced Malware Protection (AMP) и фильтрация URL-адресов. Устройства Cisco Firepower серии 2100 используют

программный образ системы защиты от угроз Cisco Firepower Threat Defense. В качестве альтернативы эти устройства могут поддерживать программный образ многофункционального устройства безопасности Cisco Adaptive Security Appliance (ASA).

Решение Cisco Firepower Management Center (ранее называлось FireSIGHT) обеспечивает централизованное управление межсетевыми экранами нового поколения Cisco Firepower NGFW, а также системами Cisco Firepower NGIPS and Cisco AMP.

Решение Cisco Firepower Device Manager доступно для локального управления устройствами серии 2100, на которых выполняется программный образ Cisco Firepower Threat Defense.

Технические параметры производительности и описание функций.

Основные параметры производительности:

- Пропускная способность FW + AVC (Cisco Firepower Threat Defense) 1,9 Гбит/с
- Пропускная способность: FW + AVC + NGIPS (Cisco Firepower Threat Defense)1 1,9 Гбит/с
- Сеансы HTTP со средним размером пакета 1024 байт
- Производительность МСЭ TCP 1024 байт.

Производительность МСЭ отличается в зависимости от характеристик сети и трафика. При использовании с новыми версиями ПО производительность может изменяться.

Cisco Firepower серии 2100 - первый в отрасли межсетевой экран нового поколения в форм-факторе 1RU обеспечивает стабильную производительность с активной функцией защиты от угроз

Таблица 1

Технические параметры производительности и описание функций при использовании образа Firepower Threat Defense

Возможности	Модель Cisco Firepower
2110	
Пропускная способность: FW + AVC1	1,9 Гбит/с
Пропускная способность: AVC + IPS1	1,9 Гбит/с
Максимальное число параллельных сеансов, с AVC	1 млн
Максимальное число новых подключений в секунду, с AVC	12 000
Cisco Firepower Device Manager (локальное управление)	Да
Централизованное управление	Централизованная конфигурация регистрация, мониторинг и отчетность выполняются решением Firepower Management Center или, в качестве альтернативного варианта, в облаке с помощью Cisco Defense Orchestrator
Мониторинг и контроль приложений (AVC)	Стандартный, поддерживает более 4000 приложений, а также геолокацию, пользователей

	и веб-сайты
AVC: Поддержка OpenAppID для настраиваемых пользователем детекторов приложений с открытым кодом	Стандартный
Cisco Security Intelligence	Стандартный, с анализом угроз IP, URL и DNS
Cisco Firepower NGIPS	Доступно; может пассивно обнаруживать оконечные устройства и инфраструктуру для корреляции угроз и анализа индикаторов компрометации (IoC).
Cisco AMP for Networks	Доступно; обеспечивает обнаружение, блокирование, отслеживание, анализ и сдерживание целенаправленного и устойчивого вредоносного ПО, действуя на всем протяжении атаки и после нее. Кроме того, дополнительно доступна интеграция функции корреляции угроз с решением Cisco AMP для оконечных устройств.
Песочница Cisco AMP Threat Grid	Доступно
Фильтрация URL-адресов: число категорий	Более 80
Фильтрация URL-адресов: число категоризированных URL-адресов	Более 280 миллионов
Автоматические обновления наборов угроз и сигнатур IPS	Да: лучшая в классе система аналитики коллективной безопасности (Collective Security Intelligence, CSI) от команды Cisco Talos (http//www cisco com/c/en/us/products/security/talos html)
Экосистема третьих фирм с открытым исходным кодом	Открытый API-интерфейс для интеграции с продуктами третьих фирм; Snort® и ресурсы сообщества OpenAppID для новых и специфических угроз.
Высокая доступность и кластеризация	Активно/в режиме ожидания; для кластеризации внутри шасси Cisco Firepower 9300, допустимо до 5 шасси; в устройствах Cisco Firepower серии 4100 допустима кластеризация до 6 шасси
Максимум сетей VLAN	1024
Технологии Cisco Trust Anchor	Устройства ASA 5506-X, 5508-X и 5516-X, платформы Firepower серии 2100, 4100 и 9300 включают технологии Trust Anchor для цепочки поставок и надежного программного образа. Более подробную информацию см. в разделе ниже.

Таблица 2

Технические характеристики аппаратного обеспечения Cisco Firepower серии 2100

Возможности	Модель Cisco Firepower
2110	
Габариты, В x Ш x Г	1,73 x 16,90 x 19,76 дюйма (4,4 x 42,9 x 50,2 мм)
Форм-фактор (RU)	1RU
Слоты для модулей безопасности	—
Слоты для модуля ввода-вывода	0
Встроенные порты ввода-вывода	12 интерфейсов 10M/100M/1GBASE-T Ethernet (RJ-45), 4 интерфейса 1 Gigabit (SFP) Ethernet
Сетевые модули	Нет
Примечание. Устройства серии 2100 можно также развертывать как выделенные сенсоры угроз с неспособными к подключению сетевыми модулями. Более подробную информацию можно узнать у представителя Cisco.	
Максимальное число интерфейсов	Всего до 16 Ethernet-портов (12 портов 1G RJ-45, порта1G SFP)
Интегрированные порты сетевого управления	1 Ethernet-порт 10M/100M/1GBASE-T (RJ-45)
Последовательный порт	1 консольный порт RJ-45
USB	1 порт USB 2.0 Type-A (500mA)
Память	1 x 100 Гбайт, 1 запасной слот (для MSP)
Источники питания Конфигурация	Одинарный встроенный блок питания переменного тока 250 Вт.
Входное напряжение в сети переменного тока	От 100 до 240 В переменного тока
Максимальный переменный ток на входе	< 2,7А при 100 В
Максимальная выходная мощность переменного тока	250 Вт
Частота переменного тока	От 50 до 60 Гц
Выход по току (переменному)	> 88% (при нагрузке 50 %)
Входное напряжение в сети постоянного тока	—
Максимальный постоянный ток на входе	—
Максимальная выходная мощность постоянного тока	—
Выход по току (постоянному)	—
Резервирование	Нет
Вентиляторы	4 встроенных (2 внутренних, 2 внешних) вентилятора2
Шум	56 дБА при 25С 74 дБА при самой высокой производительности системы
Монтаж в стойку	Да. Фиксирующие монтажные кронштейны

	включены в комплект поставки (2 шт.). Рельсы для монтажа заказываются дополнительно (4-стоечная конструкция EIA- 310-D)
Масса	< 15,4 фунтов (7,0 кг): с двумя SSD-накопителями

Сеансы HTTP со средним размером пакета 1024 байт.

Производительность отличается в зависимости от активированных функций, используемых протоколов сетевого трафика и характеристик размера пакета. При использовании с новыми версиями ПО производительность может изменяться.

Решение Cisco Firepower™ Management Center повышает эффективность решений сетевой безопасности Cisco® благодаря централизованному, интегрированному и оптимизированному управлению.

Программный продукт Cisco StealthWatch.

Система Stealthwatch® обеспечивает лучшие в отрасли возможности мониторинга сети и анализа безопасности для ускорения и более точного обнаружения угроз, реагирования на инциденты и проведения расследований.

С помощью Netflow и других телеметрических данных, полученных из существующей инфраструктуры, это решение позволяет экономически эффективно превратить всю сеть в сенсорную систему. Решение позволяет обнаруживать аномальный трафик и поведение, включая вредоносное ПО нулевого дня, распределенные атаки отказа в обслуживании (DDoS), внутренние угрозы, а также новейшие целенаправленные угрозы (APT).

Система Stealthwatch снабжена интуитивно понятным веб-интерфейсом. Она обеспечивает единое представление о горизонтальном движении трафика в сети. Кроме того, система предоставляет высокотехнологичные возможности для анализа и оповещений. Эта простая, удобная и мощная платформа расширяет возможности для использования, анализа безопасности и раннего обнаружения угроз.

Благодаря своему уникальному ракурсу и анализу сетевого трафика система Stealthwatch значительно улучшает:

- обнаружение угроз в режиме реального времени;
- реагирование на инциденты и расследования;
- сегментацию сети;
- производительность сети и планирование пропускной способности;
- возможности для обеспечения соответствия регулятивным требованиям.

Консоль управления системы Stealthwatch.

Консоль управления системы Stealthwatch Management Console обеспечивает единую точку наблюдения для распределенных ИТ-групп с возможностью просмотра контекстуальной информации обо всей активности в сети. Простой наглядный интерфейс позволяет операторам быстро находить проблемы и реагировать соответствующим образом.

Мощность консоли определяет объемом данных Netflow, которые могут быть проанализированы и отображены, а также количество сборщиков данных потока

Stealthwatch Flow Collector, которое можно развернуть. Консоль предлагается в виде аппаратного устройства или виртуальной машины.

Консоль управления Stealthwatch обеспечивает следующие основные функции:

- Отслеживание пользователей
- Гибкие возможности развертывания, включая виртуальные устройства
- Быстрый анализ основной причины и устранение неполадок
- Реляционные карты потоков
- Сшивка NAT
- Настраиваемые инструментальные панели (dashboard)
- Настраиваемые отчеты
- Автоматизированная блокировка, устранение проблем и ограничение скорости
- Отчеты типа Top-N для приложения, сервисов, портов, протоколов, узлов, одноранговых узлов и сеансов
- Разбивка трафика на составляющие
- Настраиваемый пользовательский интерфейс на базе технологии Point-of-View™
- Поддержка многогигабитных сетевых сред и крупномасштабных сетевых сред с многопротокольной коммутацией на основе меток (MPLS)
- Расширенная визуализация потока
- Массовая масштабируемость
- Комбинированный внутренний и внешний мониторинг
- Планирование пропускной способности и определение тенденций на базе исторических данных о трафике
- Отчетность об оптимизации WAN
- Использование полосы пропускания с поддержкой точки кода дифференцированных услуг (DSCP)
- Визуализация распространения червей
- Внутренняя защита для высокоскоростных сетей

Таблица 3

Основные преимущества консоли управления Stealthwatch

Преимущество	Описание
Данные в режиме реального времени с ежеминутным обновлением	Обеспечивает предоставление потока данных для одновременного мониторинга трафика через сотни сетевых сегментов для выявления подозрительного поведения сети. Эта функция особенно ценна на уровне предприятия.
Возможность обнаружения и приоритизации угроз безопасности	Быстро обнаруживает и приоритизирует угрозы безопасности, точно определяет ненадлежащее пользование сетью и неоптимальную производительность, а также управляет реагированием на события в рамках одного центра управления.
Сетевые группы	Создает сетевые группы и карты отношений для простого представления состояния трафика в организации. В течение считаных секунд рабочие группы и группы безопасности могут точно увидеть места, которые требуют их внимания.
Графическое	Обеспечивает графическое представление состояния сети в

представление	ясном и простом для понимания формате.
Быстрая оценка состояния защиты	Отображает несколько категорий оповещения на начальной инструментальной панели, чтобы операторы могли быстро оценить состояние защиты организации.
Управление устройствами Stealthwatch	Настраивает устройства Stealthwatch, координирует их и управляет ими, включая устройства Flow Collector (сборщик данных потока), Flow Sensor (сенсор потока) и IDentity.
Использование нескольких типов данных потока	Использует несколько типов данных потока, включая Netflow, экспорт информации о потоке интернет-протокола Internet Protocol Flow Information Export (IPFIX) и sFlow. Результат: экономичная защита сети на основе поведения.
Масштабируемость	Поддерживает даже самые большие потребности сети. Отлично работает в сверхбыстродействующих средах и в состоянии обеспечить защиту каждой части сети с доступностью по IP-адресу вне зависимости от размера.
Выбор методов реализации	У вас есть возможность заказать Appliance Edition — масштабируемое устройство для организаций любого размера. Кроме того, можно заказать Virtual Edition, которое разработано для выполнения тех же функций, что и Appliance Edition, но в среде VMware.
Расширенный функционал управления сетью	Обеспечивает расширение возможностей для управления сетью за счет анализа тенденции, сетевого экрана и планирования пропускной способности, а также мониторинга производительности.
Обработка угроз APT, вредоносного ПО и внутренних угроз	Обеспечивает глубокий анализ и контекст, необходимые для отражения возникающих угроз. К ним относится все, от червей, вирусов и другого вредоносного ПО до целевых атак, попыток атак DDoS, внутренних угроз и угроз APT. Обеспечивает оповещения с контекстуальной информацией, которая нужна специалистам по безопасности для принятия быстрых и решительных мер с целью предотвращения потенциального ущерба
Журналы аудита для сетевых транзакций	Обеспечивает полные журналы аудита всех сетевых транзакций для более эффективных расследований.
Настраиваемые реляционные карты потока, работающие в режиме реального времени	Обеспечивает графические представления текущего состояния трафика организации. Администраторы могут легко создавать карты своих сетей на базе любого критерия, например, местоположения, функции или виртуальной среды. Создавая соединение между двумя группами узлов, операторы могут быстро анализировать обмен трафиком между ними. Затем, просто выбрав интересующую их точку передачи данных, они могут выполнять еще более глубокий анализ того, что происходит в тот или иной момент времени.

Сенсор потока Stealthwatch Flow Sensor — это компонент, обеспечивающий создание данных Netflow для сегментов коммутирующей и маршрутизирующей

инфраструктуры, которая не поддерживает Netflow. Он также работает в средах, в которых оверлейное решение мониторинга больше подходит для операционной модели ИТ-организации. Сенсор потока может обеспечивать информацию о приложениях уровня 7 для сред, в которых не поддерживается технология распознавания приложений средствами сети Cisco® Network-Based Application Recognition (NBAR).

Сенсор потока обеспечивает комплексный мониторинг сети, а также получение показателей производительности серверов. Он объединяет глубокий анализ пакетов (DPI) с анализом поведения для определения приложений и протоколов. В результате обеспечивается оптимизированная защита, эксплуатация сети и производительность приложений.

Объем данных Netflow, созданных в сети, определяется емкостью развернутых сенсоров потока. Имеется возможность для установки нескольких сенсоров потока. Сенсоры потока предлагаются в виде аппаратных устройств или программного обеспечения для мониторинга сред на базе виртуальных машин.

Сенсор потока Stealthwatch обеспечивает следующие основные функции:

- Контекст приложения уровня 7
- Мониторинг потока
- Создание данных Netflow
- Мониторинг виртуальной среды
- Обновления в режиме реального времени для текущих угроз
- Вычисление времени передачи обоих пакетов (RTT) и времени отклика сервера (SRT) для TCP-соединений

Таблица 4

Основные преимущества сенсора потока Stealthwatch

Преимущество	Описание
Обзор приложений уровня 7	Обеспечивает мониторинг приложения уровня 7 за счет сбора информации о приложении вместе со статистикой производительности на уровне пакетов.
Производительность и анализ на уровне пакетов	Обеспечивает мониторинг приложения уровня 7 за счет сбора информации о приложении вместе со статистикой производительности на уровне пакетов.
Оповещения об аномалиях в сети	Точно определяет необычное поведение сети и немедленно отправляет оповещения с контекстуальной аналитикой для того, чтобы специалисты по безопасности могли быстро предпринять необходимые действия и предотвратить ущерб.
Снижение затрат	Повышает операционную эффективность и уменьшает затраты благодаря определению и локализации основных причин проблемы или инцидента в течение считаных секунд
Выбор методов реализации	Проектом предусмотрена поставка в виде Virtual Edition, котороя разработана для выполнения тех же функций, что и Appliance Edition, но в среде VMware.

В сетях предприятия используется 2 устройства Cisco ASA 5525.

1-ое устройство - производится перенос устройства ASA 5525 в рамках действующей сети и проводятся необходимые работы по настройке оборудования. Применяется на периметре сети ИТС и ЦОУ ДВД.

2-ое устройство Cisco ASA 5525 производится модернизация устройства до уровня Cisco ASA5525 FirePOWER, применяется на периметре сети ИТС-ЦОД.

2 устройства Cisco ASA5525 для производства работ предоставляется Заказчиком.

Устройства Cisco FirePOWER Межсетевой экран нового поколения Cisco Firepower® Next-Generation Firewall (NGFW).

Общее описание

Межсетевой экран нового поколения Cisco Firepower® Next-Generation Firewall (NGFW) – это первый в отрасли полностью интегрированный межсетевой экран нового поколения с ориентацией на защиту от угроз и с унифицированным управлением. Он обеспечивает расширенную защиту от угроз до, вовремя и после атак.

	Нейтрализация еще большего числа атак	Нейтрализация известного и неизвестного вредоносного ПО с помощью лидирующего в отрасли решения Cisco® Advanced Malware Protection (Cisco AMP) и песочницы.
	Еще лучший мониторинг	Непревзойденный мониторинг всей среды с использованием системы предотвращения вторжений нового поколения Cisco Firepower IPS. Автоматические рейтинги рисков и флаги вторжений показывают приоритеты, чтобы вашим специалистам было проще ориентироваться.
	Раннее обнаружение, быстрая реакция	Согласно данным годового отчета Cisco по безопасности среднее время от инфицирования до обнаружения составляет для предприятий в среднем 100 дней. Cisco уменьшает это время до нескольких часов.
	Уменьшение сложности	Обеспечение унифицированного управления и автоматической корреляции угроз по всем тесно интегрированным функциям безопасности, включая мониторинг и контроль приложений, NGIPS и AMP.
	Использование всего потенциала сети	Повышение безопасности и использование всех преимуществ уже сделанных инвестиций с возможностью дополнительной интеграции других решений в области безопасности и сетевых технологий как Cisco, так и третьих фирм.

Решение Cisco Firepower Management Center (ранее решение называлось FireSIGHT Management Center) — это административный центр для целого ряда продуктов безопасности Cisco, выполняемых на самых разных платформах. Решение обеспечивает полное, унифицированное управление межсетевыми экранами, контролем приложениями, предотвращением вторжений, фильтрацией URL-адресов и защитой от усовершенствованного вредоносного ПО.

Центр управления — это центральная точка для управления событиями и политиками следующих решений:

- межсетевой экран нового поколения Cisco Firepower Next-Generation Firewall (NGFW);
- Cisco ASA с сервисами FirePOWER;
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Advanced Malware Protection (AMP)

Решение Cisco Firepower Management Center позволяет получить подробную аналитическую информацию о пользователях, приложениях, устройствах, угрозах и

уязвимостях, существующих в вашей сети. Это решение использует эту информацию для анализа уязвимостей вашей сети, а затем предоставляет адаптированные рекомендации о том, какие политики безопасности следует внедрить, а какие события безопасности изучить и расследовать.

Центр управления предоставляет удобные в использовании экраны политик для контроля доступа и защиты от известных атак. Решение интегрируется с защитой от усовершенствованного вредоносного ПО и «песочницей», а также предоставляет инструменты для отслеживания инфицированного вредоносного программного обеспечения (далее по тексту ПО) по всей сети. Все эти возможности объединены в одном интерфейсе управления. Есть возможность переходить от управления межсетевым экраном к управлению приложениями или расследованию и устранению вторжений со стороны вредоносного ПО.

Управление корпоративного класса.

Cisco Firepower Management Center получает оперативную информацию обо всех изменениях сетевых ресурсов и операций и предоставляет полную контекстную базу для принятия обоснованных решений. Помимо предоставления широкого набора аналитических решений, Firepower Management Center обеспечивает высокий уровень детализации.

Таблица 5

Функции и преимущества

Функция	Преимущество
Унифицированное управление разными функциями безопасности на разных платформах	Облегчает централизованное управление средой безопасности Cisco, включающей следующие решения: • межсетевой экран нового поколения Cisco Firepower Next-Generation Firewall (NGFW); • Cisco ASA с сервисами FirePOWER; • Cisco Firepower NGIPS; • Cisco FirePOWER Threat Defense for ISR • Cisco AMP.
Интегрированное управление политиками для разных функций безопасности	Конфигурирует настройки доступа к межсетевому экрану, контроля приложений, предотвращения угроз, фильтрации URL-адресов и защиты от усовершенствованного вредоносного ПО в единой политике. Облегчает управление политиками, уменьшает количество ошибок и обеспечивает целостность и единообразие. Позволяет применять одну политику сразу к нескольким решениям по безопасности.
Интеграция управления политиками доступа с Cisco Identify Services Engine	Управляет доступом на основе меток группы безопасности ISE, типа устройств и местоположения IP, а также обеспечивает быстрое сдерживание угроз Обеспечивает соответствие нормативным требованиям, повышает безопасность инфраструктуры и оптимизирует работу сервисов

Высочайший уровень аналитики сетевых угроз	Интегрирует аналитические данные по безопасности, угрозам и уязвимостями, предоставленные группой Cisco Talos, для обеспечения защиты от угроз за считанные минуты. Использует новые методы защиты от атак на основе данных безопасности по IP- и URL-адресам включает Cisco Umbrella для мониторинга угроз за пределами периметра сети. Обеспечивает получение и сопоставление аналитических данных об угрозах из каналов данных об угрозах и платформ анализа угроз третьих сторон в форматах STIX/TAXII или простых файлов
Мониторинг и контроль приложений	Сокращает число угроз для вашей сети за счет точного контроля более 4000 коммерческих приложений. Использует OpenAppID на основе открытых стандартов для подробной идентификации и управления пользовательскими приложениями
Многопользовательское управление и наследование политик	Создает до 50 доменов управления с отдельными данными событий, отчетностью и сопоставлением сетей, реализованными через управление доступом на основе ролей. Обеспечивает целостное и эффективное управление благодаря своей иерархической структуре политик, в которой каждый уровень наследует политики вышестоящего уровня.
Отчеты и информационные панели	Обеспечивает необходимый уровень мониторинга за счет создания настраиваемых информационных панелей с пользовательскими отчетами на основе шаблонов Предоставляет всеобъемлющие отчеты и предупреждения по общим и целевым данным. Отображает контекстную информацию и информацию о событиях в виде таблиц, графиков и диаграмм с гиперссылками для удобства использования в аналитических целях Контролирует поведение сети и производительность на предмет обнаружения аномалий и поддержания работоспособности системы.
Защищенная загрузка	Защищенная загрузка (Secure boot) — это механизм для подтверждения целостности и подлинности программного обеспечения Cisco, выполняемого на оборудовании FMC при загрузке системы. Если сигнатура отсутствует, или программное обеспечение недействительно, оно не будет загружаться, и самозрагрузки системы не произойдет. (только FMC 1000, FMC 2500, FMC 4500)

Мониторинг и подробный анализ.

Решение Cisco Firepower Management Center автоматически собирает, сопоставляет и отображает контекстную информацию обо всем, что происходит в вашей среде. В таблице 6 представлен весь диапазон контекстных данных, которые можно получить о векторах угроз, и которые не в состоянии обнаружить стандартные технологии обеспечения безопасности. Такие подробные данные анализа сети можно использовать

для определения политик защиты и обеспечения такого высокого уровня защиты, которые не могут предоставить другие решения.

Таблица 6

Полная прозрачность инфраструктуры

Категория	Cisco Firepower Management Center	Обычная система обнаружения вторжений	Обычный межсетевой экран нового поколения
Угрозы	Да	Да	Да
Пользователи	Да	Да	Да
Веб-приложения	Да	Нет	Да
Протоколы приложений	Да	Нет	Да
Передача файлов	Да	Нет	Да
Вредоносное ПО	Да	Нет	Нет
Серверы команд и управления	Да	Нет	Нет
Клиентские приложения	Да	Нет	Нет
Сетевые серверы	Да	Нет	Нет
Операционные системы	Да	Нет	Нет
Маршрутизаторы и коммутаторы	Да	Нет	Нет
Мобильные устройства	Да	Нет	Нет
Принтеры	Да	Нет	Нет
Телефоны VoIP	Да	Нет	Нет
Виртуальные машины	Да	Нет	Нет
Информация об уязвимостях	Да	Нет	Нет

Управление на всем протяжении атаки — до, вовремя и после.

Решение Cisco Firepower Management обеспечивает унифицированное управление на всем протяжении атаки — до, вовремя и после.

До

Обеспечивает непревзойденный мониторинг того, что происходит в вашей сети, чтобы вы могли увидеть угрозу и принять соответствующие меры.

Создает правила для МСЭ и контролирует более 4000 коммерческих и пользовательских приложений, выполняемых в вашей среде.

Во время

Определяет уровни предотвращения вторжений, правила репутации URL-адресов и компоненты защиты от усовершенствованного вредоносного ПО, которые необходимо установить.

Применяет такие политики, как: «Если трафик приходит из этой страны с использованием этого конкретного приложения с прикрепленным файлом, я будут применять этот уровень проверки на предмет наличия вторжения и анализировать этот файл на предмет наличия вредоносного ПО, и даже, при необходимости, отправлять его в песочницу».

После

Создает графическое представление всех устройств, которые были инфицированы в результате конкретной атаки.

Обеспечивает возможность легко создавать пользовательское правило для остановки атаки и предотвращения ее распространения.

Предоставляет подробные аналитические данные о конкретном вредоносном ПО для его безопасного удаления.

Автоматическая безопасность для динамической защиты.

Решение Cisco Firepower Management Center постоянно следит за изменениями в сети, которое оптимизирует работу сети и обеспечивает ее безопасность благодаря следующим возможностям:

- Автоматическая корреляция событий новых атак с уязвимостями вашей сети для того, чтобы предупреждать вас об атаках, которые могут оказаться удачными. Ваша команда специалистов по безопасности сможет сфокусировать свое внимание на событиях, которые важнее всего;
- Анализ уязвимостей вашей сети и автоматическое предоставление рекомендаций о политиках безопасности, которые следует внедрить. Вы можете адаптировать ваши механизмы защиты к меняющимся условиям и внедрить меры безопасности, подходящие конкретно для вашей сети.

Корреляция отдельных событий из сети, оконечного устройства, системы обнаружения вторжений и анализа безопасности. В случае если отдельные узлы проявляют признаки компрометации, связанные с неизвестными атаками, вы получаете предупреждение.

Применение критериев политик. Если эти политики удовлетворены, система автоматически анализирует файл на предмет выявления известного вредоносного ПО и (или) отправляет этот файл во встроенную песочницу для определения неизвестного вредоносного ПО.

Открытые API-интерфейсы для удобной интеграции

Решение Cisco Firepower Management Center делает возможным интеграцию с технологиями третьих фирм благодаря использованию четырех прикладных программных интерфейсов с мощным и эффективным функционалом Эти API-интерфейсы представляют собой точки подключения для реализации перечисленных ниже задач.

Перемещение данных событий из решения Management Center на другую платформу, например, решение по управлению информацией и событиями безопасности (SIEM)

Пополнение информации, содержащейся в базе данных Cisco Firepower, данными третьих фирм. Такие данные могут включать данные систем управления уязвимостями и информацией об операционных системах из активных сканеров.

Запуск рабочих процессов и реализация шагов по восстановлению, которые инициируются правилами корреляции, определяемыми пользователями. Например, можно интегрировать рабочий процесс с решением контроля сетевого доступа (NAC) для помещения в карантин инфицированного оконечного устройства, или запустить процесс цифрового расследования.

Поддержка возможностей по созданию отчетности и аналитики третьих фирм благодаря предоставлению возможности этим решениям отправлять запросы в базу данных Management Center.

Эти API-интерфейсы также используются для интеграции с отдельными продуктами и рабочими операциями Cisco по обеспечению безопасности. Среди них: Cisco AMP Threat Grid для песочницы; Cisco Identity Services Engine для идентификации данных и сегментации сети и Cisco Umbrella для мониторинга доменов по всей сети Интернет.

Threat Intelligence Director

Функция Threat Intelligence Director теперь доступна в решении Cisco Firepower Management Center (v6.2.1). Используя открытые API-интерфейсы, функция Threat Intelligence Director облегчает получение аналитических данных об угрозах третьих сторон из таки источников, как каналы с данными об угрозах и платформы анализа угроз (threat intelligence platforms, TIP). Эта функция поддерживает стандарты Structured Threat Information Expression (STIX) и Trusted Automated Exchange of Indicator Information (TAXII) или отдельные форматы простых (неотформатированных) файлов. Threat Intelligence Director раскладывает получаемые аналитические данные на компоненты, которые можно изучать (IoCs), включая IP (IPv4, IPv6), домены, URL-адреса и SHA-256. Все эти данные передаются на устройства безопасности Cisco, которые могут автоматически блокировать действия злоумышленников изнутри или осуществлять мониторинг сети с целью быстрого реагирования на угрозы.

Threat Intelligence Director может обрабатывать доступные аналитические данные об угрозах для следующих устройств безопасности Cisco:

- Межсетевой экран нового поколения Cisco Firepower NGFW
- Система защита от вторжений нового поколения Cisco Firepower NGIPS

Варианты развертывания.

Решение Cisco Firepower Management Center можно развертывать как физическое или виртуальное устройство, или из облака, поэтому вы сможете выбрать тот вариант, который лучше всего подойдет для вашей среды. Физические устройства обычно могут управлять большим числом сенсоров и предоставляют больше емкости для хранения событий, чем их виртуальные аналоги. Удобство виртуальных устройств заключается в возможности использования существующей инфраструктуры виртуальных машин. Для хостинга Management Center можно также использовать облачные вычислительные сервисы. Эти сервисы обеспечиваю управление безопасностью без необходимости дополнительных инвестиций в вычислительные мощности и хранилище базы данных. Кроме того, они дают возможность гибкого и быстрого масштабирования по мере потребности.

При использовании функции Threat Intelligence Director на виртуальных МСЭ нового поколения для оптимальной производительности рекомендуется устанавливать на оборудование память объемом 15 Гбайт.

Технические характеристики платформы.

Решение Cisco Firepower Management Center предлагается в виде нескольких разных моделей. Выберите модель, наилучшим образом подходящую для вашей организации, в зависимости от количества сенсорных устройств, подлежащих мониторингу

(оба варианта - и физические, и виртуальные), числа хостов в вашей среде и ожидаемому числу событий безопасности (см. таблицу 3). Все модели предоставляют следующие одинаковые возможности управления:

- Централизованное управление устройствами, лицензиями, событиями и политиками.
- Управление на основе ролей (сегментированные и отдельные представления и обязанности в зависимости от роли администратора или группы).
- Настраиваемые информационные панели с отчетами на основе шаблонов и настраиваемые в соответствии с потребностями пользователей.
- Всеобъемлющие отчеты и предупреждения по общим и целевым данным.
- Контекстная информация и информация о событиях в виде таблиц, графиков и диаграмм с гиперссылками.
- Поведение сети и контроль производительности.
- Надежные функции высокой доступности для гарантии отсутствия сбоев
- Функции корреляции и восстановления для реагирования на угрозы в реальном времени.
- Открытые API-интерфейсы для интеграции с решениями третьих фирм и пользовательскими рабочими потоками, такими как межсетевые экраны, сетевая инфраструктура, управление журналами, SIEM, журналы неисправности и управление исправлениями.
- Платформа Cisco Identity Services Engine.

В связи с увеличением количества пользователей, устройств и методов доступа корпоративные ИТ-инфраструктуры современных предприятий становятся более динамичными. Наряду с расширением возможных вариантов подключения и спектра пользовательских устройств появляются новые риски нарушения безопасности и задачи по сохранению управляемости. Для обеспечения информационной безопасности корпоративной ИТ-инфраструктуры и эффективного управления такой инфраструктурой требуются новые решения, которые обеспечат выполнение политик доступа, аудит доступа к ИТ-инфраструктуре, мониторинг соблюдения нормативных требований, а также сбор подробных сведений о всех сетевых взаимодействиях.

Обзор продукта

Cisco Identity Services Engine является платформой следующего поколения для управления процессами идентификации и контроля доступа, которая позволяет организациям обеспечить соблюдение нормативных требований, повысить уровень защищенности корпоративной ИТ-инфраструктуры и упростить управление работой сетевых сервисов. Благодаря уникальной архитектуре решения предприятия могут в режиме реального времени получать из сетей, от пользователей и устройств контекстную информацию, необходимую для принятия упреждающих решений по предоставлению доступа. Все решения принимаются на основании единой политики доступа, распространяющейся на проводные сегменты сети, беспроводные сегменты сети и подключения удаленного доступа.

Cisco Identity Services Engine представляет собой решение для контроля доступа с учетом контекста, которое объединяет сервисы аутентификации, авторизации и учета (AAA), оценки состояния, профилирования и управления гостевым доступом в рамках

единой платформы. Администраторы получают возможность централизованно создавать согласованные политик контроля доступа и управления ими, а также полную осведомленность обо всех пользователях и устройствах, подключающихся к сети. Решение Cisco Identity Services Engine автоматически выявляет и классифицирует оконечные устройства, обеспечивает нужный уровень доступа, проводя аутентификацию как пользователей, так и устройств, а также обеспечивает соответствие оконечных устройств нормативным требованиям путем оценки их состояния защищенности перед предоставлением доступа к корпоративной ИТ-инфраструктуре. Cisco Identity Services Engine поддерживает гибкие механизмы контроля доступа, включая группы безопасности (SGA), метки групп безопасности (SGT) и списки контроля доступа групп безопасности (SGACL).

Функциональные возможности.

Платформа Cisco Identity Services Engine предоставляет следующие возможности:

- Внедрение в корпоративную ИТ-инфраструктуру средств аутентификации и авторизации пользователей и оконечных устройств, подключенных к проводным сетям, беспроводным сетям и сетям VPN, обеспечение соблюдения согласованной политики в масштабах всего предприятия.
- Предотвращение несанкционированного доступа к сети для защиты корпоративных активов.
- Управление полным жизненным циклом гостевого доступа за счет предоставления приглашающим лицам средств для разрешения доступа их гостей, что позволяет снизить текущую нагрузку на ИТ специалистов.
- Поддержка настраиваемых порталов и возможности публикации web-страниц для упрощения работы как новых, так и опытных пользователей в соответствии с принятыми в организации процессами.
- Обеспечение полномасштабного мониторинга путем обнаружения, классификации и управления подключающимися к сети оконечными устройствами для предоставления соответствующих сервисов и уровней доступа.
- Устранение уязвимостей на компьютерах пользователей путем регулярной проверки и корректировки их состояния, что позволяет нейтрализовать такие сетевые угрозы, как вирусы, черви и шпионские программы.
- Управление доступом оконечных устройств к сети с помощью сервиса защиты оконечных устройств (EPS). Сервис EPS позволяет администратору связывать оконечные устройства и действия, которые необходимо выполнить при подключении устройства (перенос в новую VLAN, возврат в исходную VLAN или полная изоляция устройства от сети), с помощью единого интерфейса.

Программный продукт Indeed PAM.

Аудит действий сотрудников ИТ службы компании, подрядчиков и удаленных сотрудников Indeed Privileged Access Manager (Indeed PAM).

Общее описание

Постоянное наращивание и усложнение IT-инфраструктуры компаний делает управление привилегированными учетными записями одной из важнейших задач информационной безопасности. Увеличивающееся количество информационных систем и разнообразие сценариев доступа к ним затрудняют решение этой задачи. Получив данные

административной учетной записи, злоумышленник может нанести предприятию намного более серьезный ущерб, чем в случае компрометации учетных данных рядового сотрудника. Административные учетные записи могут быть использованы для отключения защиты, остановки работы информационных систем и доступа к конфиденциальной информации. Защитить привилегированный доступ сложнее, решение этой проблемы невозможно с использованием общих подходов к защите учетных данных и требует применения специализированных решений.

Привилегированные пользователи.

Иметь повышенные права доступа к важной информации и критичным функциям программного обеспечения и оборудования могут различные категории как штатных, так и внешних сотрудников компании.

Администраторы информационных систем.

Каждое устройство и каждое прикладное или системное программное обеспечение имеют свои административные учетные записи. Это самая очевидная группа сотрудников привилегированного доступа, примерами таких сотрудников являются:

- Администраторы Active Directory
- Администраторы сетевого оборудования
- Администраторы баз данных
- Администраторы серверов (Windows, Unix/Linux)
- Администраторы VDI
- Бизнес-пользователи Бизнес-пользователи хоть и не обладают

административным доступом, но могут иметь широкие полномочия в рамках отдельно взятых информационных систем. Например, они могут иметь возможность выполнять денежные переводы, управлять производственным процессом и получать доступ к коммерческой тайне.

Служебные учетные записи Служебные учетные записи используются для различной автоматизации процессов. От их имени работают различные службы и демоны, скрипты и другое программное обеспечение. Про такие учетные записи легко забыть, т.к. сотрудники не используют их в явном виде каждый день. Это создает дополнительные трудности по управлению ими.

Продукт Indeed Privileged Access Manager (Indeed PAM) разработан как система управления доступом с использованием привилегированных учетных записей.

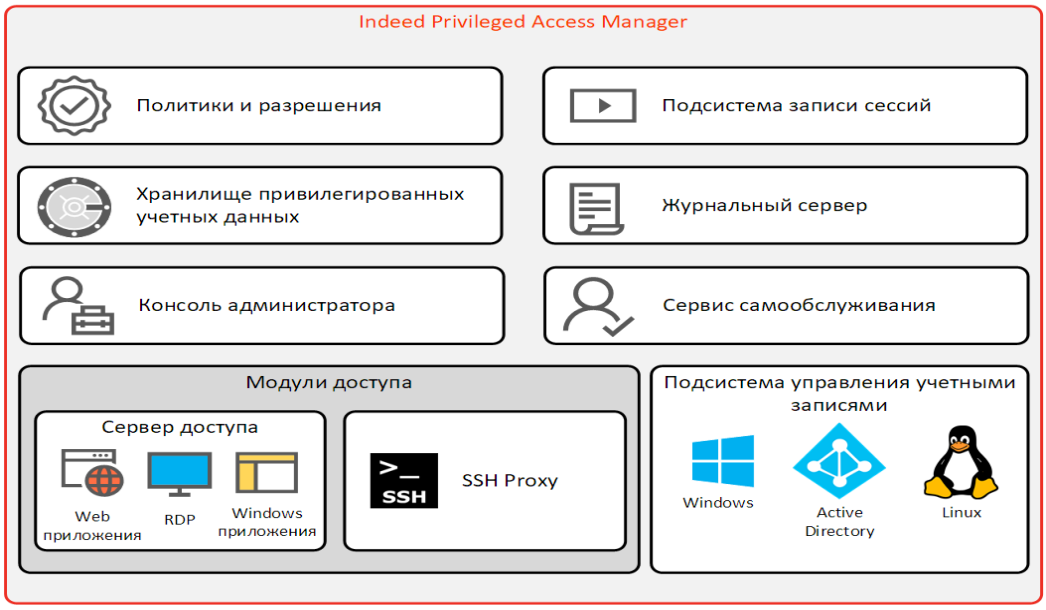

Рисунок 1. Структура Indeed Privileged Access Manager

Indeed PAM состоит из следующих функциональных и логических модулей.

Политики и разрешения определяют параметры привилегированного доступа:

кому предоставлен доступ;

- к каким учетным записям предоставлен доступ;
- к каким ресурсам (серверам и оборудованию) предоставлен доступ;
- на какое время (постоянно/временно, в рабочие часы или в любое время);
- какую запись сессий нужно производить (видео и текстовую запись, только текстовую, скриншоты и т.п.);
- какие локальные ресурсы (диски, смарт-карты) будут доступны пользователю в удаленной сессии;
- разрешено ли пользователю просматривать пароль привилегированной учетной записи Централизованные политики сокращают затраты на администрирование системы и делают параметры и права доступа прозрачными для специалистов информационной безопасности и аудиторов.

Хранилище привилегированных учетных данных

Учетные данные, необходимые для доступа (логины, пароли, SSH-ключ) хранятся в хранилище, к которому имеет доступ только сервер Indeed PAM. Хранение и передача данных к/от сервера производится в зашифрованном виде с применением стойких алгоритмов шифрования. Доступ к хранилищу ограничен и возможен только для сервера PAM, для реализации этого подхода применяется специальная процедура по “запечатыванию” сервера - hardening сервера базы данных.

Подсистема записи сессий.

Все сеансы привилегированного доступа записываются в обязательном порядке и сохраняются в архиве Indeed PAM. В архиве записи хранятся в зашифрованном виде, получить к ним доступ возможно только обладая соответствующими полномочиями в рамках системы PAM. Записи ведутся в следующих форматах:

- Текстовая запись ведется всегда и фиксирует такие данные:

1. полный ввод и вывод консоли в SSH подключениях;
2. все запускаемые процессы, открываемые окна и клавиатурный ввод для RDP подключений.

- Видеозапись производится как для RDP, так и для SSH подключений. Видеозапись не обязательна, ее включение выполняется администратором PAM с помощью механизма политик. Качество видео настраивается и может быть разным для различных учетных записей, например, сеансы администраторов домена могут записываться с максимальным качеством, а сеансы операторов со сжатием.

Снятие снимков экрана также производится как для RDP, так и для SSH подключений.

Сохранение снимков экрана не обязательно, его включение выполняется администратором PAM с помощью механизма политик. Частота снятия и качество снимков экрана задается в политиках.

Просмотр активных сессий доступен в режиме реального времени с возможностью разрыва сессии администратором PAM.

Журнальный сервер.

Журнальный сервер является выделенным сервисом по сбору событий Indeed PAM. Такие события включают в себя всю активность администраторов и пользователей PAM. Журнал фиксирует кто и какие параметры системы изменял, и кто под какими учетными данными выполнял подключение к целевым ресурсам.

Для удобства интеграции в SEIM и своевременного реагирования на инциденты, события могут доставляться по протоколу syslog на сторонний журнальный сервер.

Консоль администратора.

Консоль администратора предоставляет интерфейс для настройки, управления и аудита работы системы и выполнена в виде web-приложения. Используя консоль, администратор предоставляет пользователям доступ к учетным данным, настраивает политики доступа и просматривает журналы событий и записи привилегированных сессий. Также консоль позволяет администраторам PAM просматривать активные привилегированные сессии в реальном времени и, при необходимости, прекращать сеанс работы сотрудника. Доступ в консоль администратора выполняется с помощью двухфакторной аутентификации.

Сервисы самообслуживания

Для получения привилегированного доступа сотрудники используют два инструмента:

Консоль пользователя, выполненная в виде web-приложения. В консоли пользователя сотрудники просматривают доступные им учетные записи и ресурсы, а также запускают привилегированные сессии.

Приложение на сервере доступе. С использованием этого приложения сотрудники получают доступ минуя консоль пользователя. В этом случае сотрудник подключается напрямую к серверу доступа, где ему предлагается выбрать разрешенное подключение.

В обоих случаях доступ сотрудников защищен двухфакторной аутентификацией с помощью OTP (One-Time Password).

Модули доступа предоставляют механизмы открытия и записи привилегированных сессий.

Сервер доступа реализует централизованную модель получения привилегированного доступа. Сотрудник сначала выполняет подключение к серверу доступа, на котором проверяются его права и выполняется аутентификация по второму фактору, после чего, сотруднику открывается сессия на целевом ресурсе.

Сервер доступа работает на базе сервера удаленных рабочих столов Microsoft RDS (Remote Desktop Services), на котором установлено приложение Indeed PAM.

Данное приложение выполняет следующие функции:

- проверяет права доступа пользователя - разрешено ли ему получать доступ под запрашиваемой учетной записью на запрашиваемый целевой ресурс;
- производит аутентификацию пользователя - перед открытием сессии пользователь обязан предоставить второй фактор аутентификации;
- ведет видеозапись сессии и снятие снимков экрана.

Для открытия сессий в целевые системы и приложения на сервере доступа применяются следующее клиентское ПО:

- RDP-клиент Microsoft (mstsc) для доступа на Windows сервера;
- Браузер для доступа в web-приложения;
- SSH-клиент PuTTY для доступа на Linux/Unix системы.
- SSH Proxy
- SSH Proxy является альтернативным вариантом получения доступа через Indeed PAM в Linux/Unix системы. Данный метод обладает следующими преимуществами:
- не требуется использование Microsoft RDS;
- возможно использование любого SSH-клиента;
- SSH-клиент работает локально на рабочей станции сотрудника.
- SSH Proxy выполняет те же функции, что и сервер доступа:
- проверяет права доступа пользователя;
- производит аутентификацию пользователя;
- ведет видеозапись сессии и снятие снимков экрана.

При использовании SSH Proxy пользователь инициирует подключение со своего рабочего места с помощью привычного для него SSH-клиента. В качестве сервера подключения сотрудник указывает адрес SSH Proxy. При подключении к прокси у пользователя также запрашивается второй фактор аутентификации, после чего открывается сессия на целевой ресурс.

Подсистема управления учетными записями.

При использовании систем класса PAM офицерам информационной безопасности важно понимать, что в инфраструктуре компании нет неучтенных привилегированных записей и доступ к ним контролируется и протоколируется. В рамках Indeed PAM эту задачу решает подсистема управления учетными записями.

Подсистема выполняет следующие функции:

1. Периодический поиск новых привилегированных учетных записей на целевых ресурсах. Данная мера позволяет защититься от недобросовестного администратора, который создал себе учетную запись для работы в обход системы PAM.

2. Периодическая проверка паролей и SSH-ключей привилегированных учетных записей. Данная функция позволяет убедиться, что в хранилище PAM содержатся актуальные учетные данные и недобросовестный администратор не выполнил сброс пароля учетной записи для использования ее в обход PAM.

3. Периодическая смена паролей и SSH-ключей. Indeed PAM генерирует случайные сложные пароли и SSH-ключи для контролируемых привилегированных учетных данных, защищая их от несанкционированного доступа.

Сброс пароля учетной записи после показа его пользователю. Администратор PAM может разрешить сотрудники просматривать пароль привилегированной учетной записи в тех случаях, когда необходимо явное использование пароля. После того, как сотрудник получит пароль, через заданный промежуток времени Indeed PAM сбросит пароль в новое случайное значение.

Для выполнения указанных функций в состав подсистемы управления учетными записями входят модули подключения (коннекторы) для целевых систем:

- коннектор к Active Directory;
- коннектор к Windows и Windows Server;
- SSH-коннектор для подключения к Linux/Unix системам на базе различных дистрибутивов.
- Основные характеристики Indeed PAM
- Протоколы доступа
- RDP, SSH, HTTP(s)
- Поддерживаемые типы учетных данных
- Имя пользователя + пароль, SSH-ключи
- Поиск привилегированных учетных записей и управление паролем
- Windows, Linux, Active Directory
- Поддерживаемые каталоги пользователей
- Active Directory
- Технологии двухфакторной аутентификации
- Пароль + TOTP (программный генератор)
- Поддерживаемые типы записи сессий
- Текстовый лог. Видеозапись. Снимки экрана
- Технологии удаленного доступа
- Microsoft RDS. SSH Proxy

Двухфакторная аутентификация администраторов.

Защита доступа в Indeed Privileged Access Manager

Решения класса Privileged Access Management позволяют исключить явное использование паролей привилегированных учетных записей и гранулярно выдавать права администраторам на использование таких паролей на конкретных ресурсах. Другая проблема, которую требуются решить в части предоставления привилегированного доступа - надежная аутентификация администраторов. Перед тем, как администратор получит доступ к сессии с повышенными привилегиями, он должен быть однозначно аутентифицирован. Эту задачу решает двухфакторная аутентификация пользователей PAM.

Описание задачи

В общем виде задачу аутентификации в PAM можно сформулировать следующим образом: необходимо обеспечить возможность мультифакторной аутентификации пользователей перед предоставлением им привилегированного доступа.

Решение

Для решения описанной задачи в программном комплексе Indeed Privileged Access Manager (Indeed PAM) применяется сервер аутентификации. Сервер аутентификации Indeed PAM обладает следующими характеристиками.

Аутентификация пользователей PAM

● Двухфакторная аутентификация пользователей с применением пароля и OTP (One-Time Password)

● Возможность интеграции с Indeed Access Manager для делегирования процедуры аутентификации пользователей.

Общая архитектурная схема Indeed PAM для решения задачи аутентификации представлена в разделе 4.3

Решение задачи управления паролями в Indeed PAM обеспечивают следующие модули.

Indeed PAM Server

Центральный компонент инфраструктуры Indeed PAM. Представляет собой web-приложение, работающее на сервере Internet Information Services (IIS). Indeed PAM сервер обеспечивает централизованное управление пользователями системы, учетными данными и политиками доступа.

Сервер аутентификации

Сервер предоставляет другим компонентам решения (консоли пользователя и серверу доступа) сервис двухфакторной аутентификации пользователей. Также сервер аутентификации реализует пользовательский интерфейс аутентификации и регистрации аутентификационных данных.

Сервер доступа

Сервер доступа является центральным звеном в схеме получения привилегированного доступа. Сервер обеспечивает соблюдение политик доступа, открывает административную сессию на целевом ресурсе и ведет текстовую и видео запись сессий. Также на сервере доступа выполняется двухфакторная аутентификация перед открытием привилегированной сессии.

Консоль пользователя

В консоли пользователя сотрудники могут просмотреть доступные им учетные записи и ресурсы, а также запустить из консоли привилегированную сессию. Консоль пользователя выполнена в виде web-приложения.

Запись действий администраторов

Видео и текстовая запись сессий привилегированных пользователей

Привилегированные учетные записи несут в себе серьезные риски информационной безопасности:компрометация или злоупотребление привилегированным доступом может приводить к крупным финансовым и репутационным потерям компании. Решения класса Privileged Access Management позволяют организовать управление паролями административных учетных записей и скрыть их от сотрудников. Но одного управления паролями недостаточно, т.к. оно не решает проблемы злоупотребления привилегированным доступом. Необходимо чтобы каждый сеанс доступа оставлял цифровой “след”, который поможет расследовать инциденты и найти источник проблемы. Таким “следом” служит запись сессий. Имея архив записей, можно узнать кем, где и какие действия были произведены.

Описание задачи

Задачи по записи сессий использования привилегированных учетных записей можно сформулировать следующим образом:

1. Обеспечить видеозапись сессий.
2. Обеспечить текстовую запись сессий, в которой должны фиксироваться все запускаемые процессы и клавиатурный ввод.
3. Сохранять записи сессий в архиве, с указанием какой пользователь, под какой учетной записью и на каком ресурсе (сервере) выполнял действия.

Решение

Для решения перечисленных задач в программном комплексе Indeed Privileged Access Manager (Indeed PAM) применяется модуль записи сессий. Модуль выполняет запись и централизованно хранит архив привилегированных сессий.

Модуль записи сессий Indeed PAM обладает следующими характеристиками:

- Видеозапись сессий с возможностью настройки качества видео
- Периодическое снятие скриншотов сессий с возможностью настройки качество изображений
- Все виды записи (видео, текст, скриншоты) поддерживаются как для RDP, так и для SSH подключений.

Решение задачи управления паролями в Indeed PAM обеспечивают следующие модули.

Indeed PAM Server

Центральный компонент инфраструктуры Indeed PAM. Представляет собой web-приложение, работающее на сервере Internet Information Services (IIS). Indeed PAM сервер обеспечивает централизованное управление пользователями системы, учетными данными и политиками доступа.

Сервер доступа

Сервер доступа является центральным звеном в схеме получения привилегированного доступа. Сервер обеспечивает соблюдение политик доступа, открывает административную сессию на целевом ресурсе и ведет текстовую и видео запись сессий.

Консоль администратора

Консоль администратора предоставляет интерфейс для настройки, управления и аудита работы системы. Используя консоль, администратор предоставляет пользователям доступ к учетным данным, настраивает политики доступа и просматривает журналы событий и записи привилегированных сессий. Консоль администратора выполнена в виде web-приложения.

Видеоархив сессий

Indeed PAM производит видеозапись привилегированных сессий. Все записи сохраняются в централизованном архиве и доступны администратору для просмотра в его консоли. Помимо видеозаписи, Indeed PAM может выполнять снятие скриншотов с экрана пользователя для формирования фотоархива сессии. Видеозапись сессий ведется для всех типов сессий (RDP, SSH).

Текстовый архив сессий

Indeed PAM производит текстовую запись всех типов сессий (RDP, SSH). Записи сохраняются в архиве и доступны для просмотра и поиска в консоли администратора.

Архив снимков экрана

Indeed PAM производит периодическое снятие изображений экрана (скриншотов). Изображения сохраняются в архиве и доступны для просмотра в консоли администратора.

Управление паролями административных учетных записей

Привилегированные учетные записи несут в себе серьезные риски информационной безопасности: компрометация привилегированного доступа может приводить к крупным финансовым и репутационным потерям компании. При этом для административных учетных записей в большинстве случаев применяется парольная аутентификация, имеющая очевидные недостатки: возможность подбора паролей, возможность несанкционированной передачи паролей, необходимость своевременной смены паролей при увольнении сотрудников. Наличие таких проблем в отношении административного доступа создает угрозы безопасности компании, для их устранения необходимо использовать специализированные средства класса Privileged Access Management. Первым шагом в решении проблемы является реализация автоматического управления паролями привилегированных учетных записей.

Описание задачи

Задачи по управлению паролями привилегированных учетных записей можно сформулировать следующим образом:

1. Скрытие паролей от сотрудников, то есть возможность выдать административный доступ без раскрытия пароля.

2. Автоматическая регулярная смена паролей на случайное значение. Данная мера позволит повысить безопасность и снизить риски использования пароля в явном виде.

3. Возможность гранулярно выдавать доступ и отзывать его в любой момент. Должна быть возможность предоставить административный доступ только к явно указанным серверам.

Функции управления паролями

Предоставление административного доступа (сессии) без раскрытия пароля привилегированной учетной записи

Регулярная смена паролей привилегированных учетных записей

Возможность выдать доступ только к определенным ресурсам (серверам)

Поддерживаемые типы учетных записей

Microsoft Active Directory

Учетные записи ОС Windows

Учетные записи ОС Linux (пароли и SSH-ключи)

Учетные записи для доступа к сетевому оборудованию

Поддерживаемые протоколы доступа

RDP

SSH

Поиск привилегированных учетных записей

В состав Indeed PAM входит модуль, который выполняет поиск привилегированных учетных записей, регистрирует их в системе и предлагает взять их под контроль.

Регулярная автоматическая смена паролей привилегированных учетных записей

Indeed PAM выполняет регулярную смену паролей на случайное значение, исполняя требования как к сложности паролей, так и периодичности их смены.

Центральный компонент инфраструктуры Indeed PAM. Представляет собой web-приложение, работающее на сервере Internet Information Services (IIS). Indeed PAM сервер обеспечивает централизованное управление пользователями системы, учетными данными и политиками доступа.

Сервер аутентификации

Сервер предоставляет другим компонентам решения (консоли пользователя и серверу доступа) сервис двухфакторной аутентификации пользователей. Также сервер аутентификации реализует пользовательский интерфейс аутентификации и регистрации аутентификационных данных.

Сервер доступа

Сервер доступа является центральным звеном в схеме получения привилегированного доступа. Сервер обеспечивает соблюдение политик доступа, открывает административную сессию на целевом ресурсе и ведет текстовую и видео запись сессий. Также на сервере доступа выполняется двухфакторная аутентификация перед открытием привилегированной сессии.

Консоль пользователя

В консоли пользователя сотрудники могут просмотреть доступные им учетные записи и ресурсы, а также запустить из консоли привилегированную сессию. Консоль пользователя выполнена в виде web-приложения.

Маршрутизатор CISCO ASR1001-X

Маршрутизаторы серии Cisco ASR 1000 Aggregation Services Routers

Серия маршрутизаторов Cisco ASR 1000 - это новое поколение сервисных маршрутизаторов Cisco, разработанных для построения сетей связи нового поколения (IP NGN). Маршрутизаторы серии Cisco ASR 1000 имеют лучшее соотношение цена/производительность, высокую гибкость для организации расширенных сервисов, масштабируемую подсистему управления, а также модульность конструкции, которая делает возможным постепенное наращивание производительности по мере роста с максимальным сохранением сделанных ранее инвестиций.

Основные достоинства:

Функции для эффективного внедрения новых комплексных услуг для домашних и бизнес абонентов.

Функционал агрегации трафика сетей широкополосного доступа, интеллектуальной маршрутизации в корпоративных сетях и пограничной маршрутизации в сетях операторов связи.

Снижение операционных расходов и капиталовложений за счет быстрого развертывания новых управляемых сервисов на базе унифицированных архитектур и операционных сред.

Лучшая в отрасли производительность и интеллектуальные сервисы по беспрецедентно низкой цене.

Архитектура Cisco ASR 1000 обеспечивает полное резервирование, как аппаратных, так и программных компонентов маршрутизатора в случае сбоев.

Маршрутизаторы Cisco ASR 1000 предоставляют множество различных сервисов на скоростях от 2.5 до 200 Гбит/сек с помощью процессора Cisco Quantum Flow Processor (QFP). Сервисы включают в себя: безопасность (например, шифрование и брандмауэр), обеспечение качества обслуживания (QoS), анализ сетевых протоколов и приложений Cisco Network Based Application Recognition (NBAR) и Cisco Flexible Packet Matching (FPM), агрегация широкополосных абонентов (BRAS), пограничный контроллера соединений (SBC) и многие другие.

Благодаря архитектуре с физическим разделением плоскостей управления (control plane) и коммутации (forwarding plane), появилась возможность обеспечить резервирование на программном уровне (software redundancy) для моделей Cisco ASR 1001, ASR 1002-Fixed, ASR 1002 и ASR 1004, а также аппаратное резервирование для маршрутизаторов Cisco ASR 1006 и ASR 1013.

Маршрутизаторы серии Cisco ASR 1000 используют новую модульную операционную систему Cisco IOS XE. ОС обеспечивает высокую надежность, скорость, возможность модульной компоновки и возможность модернизации программного обеспечения маршрутизатора без остановки коммутации трафика (In Service Software Upgrade – ISSU).

Продуктовая линейка маршрутизаторов Cisco ASR 1000 состоит из шести моделей: ASR 1001, ASR 1002-X, ASR 1004, ASR 1006 и ASR 1013, в каждом из которых используется новый мощный сетевой процессор - Cisco Quantum Flow Processor.

Компоненты маршрутизаторов Cisco ASR 1000.

Маршрутизаторы Cisco ASR 1000 построены по централизованной архитектуре, в которой Route Processor (RP) выполняет функции подготовки маршрутной информации (control plane), а Embedded Service Processors (ESP) выполняет функции обработки

трафика (data-plane) на основе маршрутной информации, полученной от RP. Весь сетевой трафик устройства проходит через ESP. В слоты устройства устанавливаются модули SIP. Модуль SIP обеспечивает установку в маршрутизатор порт адаптеров SPA (Shared Port Adapter) содержащих физические интерфейсы. После попадания трафика на ESP он поступает на обработку к процессору Cisco Packet Processor (CPP), расположенному на ESP, на котором выполняются функции коммутации и иерархического QoS

Управляющий процессор (control plane) Route Processor 1 (RP1) первого поколения предназначен для работы в больших распределенных IP/MPLS сетях операторов связи и обеспечивает управление и мониторинг всех компонентов маршрутизатора.

Управляющий процессор Route Processor 2 (RP2) второго поколения наследует всю функциональность RP1, поддерживает до 16 GB оперативной памяти, использует 64-битную версию ОС. RP2 рекомендуется для применения там, где требуется быстрая и масштабируемая подсистема управления, например, в таких приложениях как BGP Route Reflector, BNG, Unified SBC.

Некоторые задачи управляющего процессора RP:

Платформа для работы модульной ОС Cisco IOS® XE.

Управление аппаратным резервированием RP, а также программным резервированием (Dual Cisco IOS) в случае использования только одного RP в шасси без остановки коммутации трафика.

Администрирование маршрутизатора – консольный, Ethernet и USB порты для настройки и обслуживания маршрутизатора.

Построение таблицы коммутации трафика и выгрузка ее в сервисный процессор Cisco ASR 1000 Series Embedded Services Processor (ESP) производящий саму коммутацию трафика.

Функции SBC – управление установлением и закрытием сессий и программирование сервисного процессора ESP для применения различных политик к голосовому и видео трафику, проходящему через маршрутизатор.

Конфигурация политик контроля доступа (stateful firewall) с последующей их передачей для исполнения на сервисный процессор ESP.

Контроль параметров: напряжение питания, температура, скорость вращения вентиляторов Сервисный процессор Cisco® ASR 1000 Series Embedded Service Processors (ESP) выполняет функции коммутации пакетов (data-plane).

Сервисный процессор выполняет все основные функции по коммутации пакетов, включая MAC classification, коммутацию на 2-ом и 3-ем уровне, обеспечение качества обслуживания (QoS) – классификацию, policing и shaping, списки контроля доступа (ACLs), VPN, балансировку нагрузки и NetFlow. ESP также выполняет функции межсетевого экрана (firewall), системы предотвращения вторжений (IPS), распознавания трафика приложений Network Based Application Recognition (NBAR) и flexible pattern matching (FPM), трансляции адресов (NAT) и др. Существует несколько моделей ESP отличающихся производительность: ESP-10, ESP-20, ESP-40, ESP-100, ESP-200.

Модуль SIP (SPA Interface Processor) для Cisco ASR 1000 обеспечивает установку в маршрутизатор порт адаптеров SPA (Shared Port Adapter) содержащих физические интерфейсы. В один модуль SIP может быть установлено до 4-х порт-адаптеров SPA одинарной высоты и до 2-х порт-адаптеров SPA двойной высоты. Модуль SIP обеспечивает классификацию входящего трафика и его буферизацию до момента

передачи трафика в ESP для обработки. Модуль SIP имеет встроенную шину синхронизации (clock) для получения и распределения синхросигналов между RP и портадаптерами SPA.

Типы шасси, типы поддерживаемых сервисных процессоров и полоса пропускания приведены в таблице в конце документа.

Порт-адаптеры SPA содержат различные физические интерфейсы для подключения маршрутизатора в сеть. Порт-адаптеры SPA взаимозаменяемы между платформами маршрутизации Cisco (например, 7600, XR-12000, CRS-1). Маршрутизаторы серии Cisco ASR 1000 поддерживают порт-адаптеры SPA.

Типы SPA:
Ethernet:
4, 8 Fast Ethernet
2 Gigabit Ethernet с поддержкой Sync Ethernet
2, 5, 8, 10 Gigabit Ethernet • 1 10Gigabit Ethernet
Serial:
2, 4 T3/E3 • 4 Serial
ATM:
• 1, 3 OC-3/STM-1 ATM
• 1 OC-12/STM-4 ATM
Channelized:
8 Channelized T1/E1
2, 4 Channelized T3
1 Channelized STM-1/OC-3
1 Channelized STM-4/OC12 (двойной высоты)
POS:
• 2, 4, 8 OC-3c/STM-1
• 1, 2, 4, 8 OC-12c/STM-4
• 1, 2, 4 OC-48c/STM-16 • 1 OC-192c/STM-64c
Webex: Webex Node SPA

Таблица 7

Характеристики маршрутизаторов серии ASR 1000:

Модель	ASR 1001
Высота шасси в RU	1
Кол-во слотов для установки RP	Интегрированный RP
Поддерживаемые типы RP	Интегрированный, на базе Intel Duo Core
Размер DRAM в RP	4Gb - 8Gb
Кол-во слотов для установки ESP	ESP Интегрирован
Тип ESP и полоса пропускания	От 2.5Гбит/с до 5 Гбит/с, апгрейд с помощью лицензии
Кол-во модулей SIP SIP-10 (10Гбит/с) SIP-40 (40Гбит/с)	1 Интегрированный SIP-10
Кол-во слотов для SPA	1

Резервирование плоскости управления	Программное
Встроенные порты GE	4
Электропитание	2 блока питания DC или AC, Резервирование 1:1

Технические требования к оборудованию Stealthwatch.

Серверное оборудование для продуктов CISCO (4xIntel 6230 2.1GHz/125W 20C/27.50MB DCP DDR4 2933 MHz, 16x16GB DDR4-2933-MHz RDIMM/1Rx4/1.2v, 8x1.2 TB 12G SAS 10K RPM SFF HDD)

Технические требования к оборудованию Indeed PUM

Серверное оборудование для Indeed PUM (2x2.2 GHz 5120/105W 14C/19.25MB Cache/DDR4 2400MHz, 8x16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v, 2x1.8TB 12G SAS 10K RPM LFF HDD (4K), 4 TB 12G SAS 7.2K RPM LFF HDD)

Среда виртуализации VMware vSphere 6 Standard

Описание к структурной схеме сети ИТС.

Программно-аппаратный комплекс защиты периметра сети ИТС Cisco Firepower 2110. Разработан для предприятий, имеющих дело с большим количеством конфиденциальных транзакций, таких как банки и розничные сети. Для повышения уровня отказоустойчивости предусмотрена поставка двух комплексов.

Программный продукт для выявления аномалий сетевого трафика Продукт с помощью телеметрических данных, полученных из существующей инфраструктуры, позволяет эффективно превратить всю сеть в сенсорную систему. Решение позволяет обнаруживать аномальный трафик и поведение, включая вредоносное ПО нулевого дня, распределенные атаки отказа в обслуживании (DDoS), внутренние угрозы, а также новейшие целенаправленные угрозы (APT).

Производится апгрейд устройства, проводятся необходимые работы по настройке оборудования. Устройство предоставляется заказчиком.

Программный продукт для контроля доступа к корпоративной сети Cisco ISE. Внедрение системы контроля доступа к сети предприятия позволит значительно снизить риски реализации угроз информационной безопасности. Продукт позволяет закрыть большой спектр вопросов контроля доступа к корпоративной сети, обеспечить централизацию политик доступа к сети.

Программный продукт по проверке соответствия требованиям Positive Technology, MaxPatrol 8 Продукт позволяет получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений. Механизмы тестирования на проникновение (Pentest), системных проверок (Audit) и контроля соответствия стандартам (Compliance) в сочетании с поддержкой анализа различных операционных систем, СУБД и Web-приложений позволяют MaxPatrol 8 обеспечивать непрерывный технический аудит безопасности на всех уровнях информационной системы. С целью максимального использования, имеющегося у заказчика серверного оборудования расчетом не предусмотрена его поставка

Программный продукт FortiClient является системой защиты конечных точек сети – рабочих станций. Antivirus обеспечивает защиту от последних вирусов, шпионского ПО и прочих угроз на уровне содержимого. Имеется у заказчика.

Программный продукт для контроля за действиями привилегированных пользователей Indeed PAM. Контроль действий лиц, сторонних пользователей, обладающих учетными записями с привилегированными полномочиями и штатных ИТ-специалистов самой компании данный продукт, обеспечивает единую точку входа, записывает все действия привилегированных пользователей в обслуживаемых системах для последующего контроля и анализа.

Маршрутизатор CISCO ASR1001-X.

Оборудование предназначено для увеличения количества внешних подключения с использованием технологии VPDN до 4 000. Через данное оборудование осуществляется взаимодействие со всеми внешними источниками начиная от автобусов заканчивая подрядными организациями

Сеть передачи данных ИТС, технологическая сеть, обеспечивающая взаимодействие различных систем.

Производится перенос устройства ASA 5525 в рамках действующей сети и проводятся необходимые работы по настройке оборудования. Устройство предоставляется заказчиком.

В рамках проектирования предусмотрено:

- Проведение изыскательских работ для выбора места установки уличных телекоммуникационных шкафов, во избежание наложения телефонной канализации с магистральным кабелем на существующие сети водопровода, бытовой и ливневой канализации, сетей тепло и электроснабжения;
- Строительство магистральных ВОЛС с применением волоконно-оптического кабеля емкостью 24 ОВ между уличными телекоммуникационными шкафами с активным оборудованием (местоположение определено исходя из характеристик оборудования);
- Строительство распределительных ВОЛС с применением волоконно-оптического кабеля емкостью 24;
- Для прокладки использован тип кабеля с броней из алюминиевой гофрированной ленты;
- Используемые оптические муфты типа МТОК-Г3/216;
- Среднеарифметическое значение затухания на сросте ОВ в муфте при измерениях с двух сторон не превышает 0,1 дБ;
- Технологический запас ВОК в телефонном колодце - 7 метров с каждой стороны муфты;
- Для подключения светофорного контроллера использован кабель емкостью 8 волокон;
- Весь прокладываемый кабель промаркирован по согласованию с Заказчиком;
- При строительстве применены оптические кроссы, предназначенные для строительства и эксплуатации городских оптических линий связи и имеющие сертификаты соответствия Республики Казахстан;
- Шкаф оборудован собственным контуром заземления;
- Исполнение шкафа уличное, с обогревом/кондиционированием для работы при внешней температуре среды от -40 до +60 градусов по Цельсию.
- При установке шкафа проложено 3 п/э трубы SDR11 д110 мм;

- Для шкафов предусмотрено обустройство бетонного основания 1500 на 2000 мм, высотой 150 мм от земли;
- Электроснабжение осуществлено от ближайшей подстанции;
- Время автономной работы при отключении электроснабжения минимум 6 часов;
- Оборудование сети DWDM имеет 2 порта Up Link 10G и не менее 16 портов 1G (резервирование 1+1). Предусмотрена установка пассивного волнового мультиплексора (4-8) портов;
- В шкафах светофорных контроллеров, подключаемых к магистральным ВОЛС, установлены 8 портовые коммутаторы (L2, L3) Fast Ethernet с поддержкой PoE 30W;
- В здании ЦУТ предусмотрена установка оборудования первичного мультиплексирования, оборудование коммутации и маршрутизации, а также усилители сигнала;
- В здании ЦУТ предусмотрена установка помимо оборудования коммутации для сети ITS, оборудование коммутации и маршрутизации для предоставления вторичных услуг по независимым каналам;
- Предусмотрено резервирование каналов, позволяющее обеспечить работоспособность кольцевой структуры при обрыве оптического кабеля с одной стороны, а также в случае отключения электричества на трех независимых объектах в одной кольцевой структуре. В кольцевой структуре не нарушатся оптическая связь при отключении одной или нескольких нод по электропитанию;
- Светофорные объекты по «малым» кольцам подключены между собой выделенным оптико-волоконным кабелем емкостью 24 волокна;
- В шкафу с установленным оборудованием DWDM предусмотрена установка коммутатора L2, L3 с модульной структурой и минимальной конфигурацией 16 портов SFP. Коммутатор поддерживает мониторинг качества предоставляемых услуг, возможность регулирования скорости передачи по порту от 10Мби/с до 1 Гбит/с с шагом 5-10Мбит/с.

Краткое описание объектов строительства.

Внедрение ITS предусмотрено применением периферийного оборудования (радиолокационные и инфракрасные транспортные детекторы, подвижные и неподвижные камеры видеонаблюдения), устанавливаемые на имеющиеся опоры и консоли светофорных объектов, а также на специально поставляемые металлические опоры.

Периферийное оборудование ITS с использованием скрытых подземных коммуникаций и воздушных линий подключены к ближайшим точкам существующих и строящихся волоконно-оптическим линиям связи (ВОЛС), городской электрической сети.

Для оптимизации процесса управления общественным транспортом в городе Нур-Султан в салонах автомобилей предусмотрено специализированное оборудование учета электронных форм проездных билетов.

В административном здании Центра управления транспортом (ЦУТ) установлено серверное оборудование с предустановленным специализированным программным обеспечением ITS, активное и пассивное сетевое оборудование, оборудование автоматизированных рабочих мест (АРМ) операторов ЦУТ.

Периферийное и мобильное (общественного транспорта) оборудование с использованием ВОЛС и средств радиосвязи вступают в информационное взаимодействие с системой ITS в ЦУТ.

Условия района строительства, адресная программа.

Периферийное оборудование детектирования и управления транспортом, видеонаблюдения предусмотрено на поставляемых металлических конструкциях (опоры, консоли) на перекрестках улиц города Астаны согласно адресной программе.

Периферийное оборудование остановочных пунктов общественного транспорта (информационные табло, смотровые видеокамеры, всепогодные шкафы для коммуникационного оборудования) предусмотрено на поставляемых специальных опорах согласно адресной программе:

Адресная программа перекрестков, оборудуемых системой ITS.
Адаптивное регулирование светофорными объектами.

№	Наименование перекрестка
1	пр.Тлендиева-ул.Бекетай
2	пр.Тлендиева-ул.Сарыбулакская
3	пр.Тлендиева-ППС
4	пр.Тлендиева-ул.Московская
5	пр.Тлендиева-ул.Акан Сери
6	пр.Женис-ул.Московская
7	пр.Женис-ПК20+22
8	пр.Женис-ул.Молдагуловой
9	пр.Женис-ул.Алтынсарина
10	пр.Женис-ул.Есенберлина
11	пр.Биржан Сал-ул.Тынышпаева
12	пр.Республики-ул.Дукенулы
13	пр.Республики- пр.Богенбай Батыра
14	ул.Бейбитшилик- пр.Богенбай Батыра
15	ул.Ауэзова-пр.Богенбай Батыра
16	ул.Айманова-пр.Богенбай Батыра
17	ул.Валиханова- пр.Богенбай Батыра
18	пр.Республики- ул.Джангильдина
19	пр.Республики- ул.Сейфуллина
20	пр.Республики-пр. Абая
21	пр.Республики- ул.Кенесары
22	пр.Республики- ул.Иманова
23	пр.Республики- "Талисман"
24	пр.Республики - "Есиль"
25	пр.Тауельсыздык- ул.Мунайтпасова
26	пр.Тауельсыздык- ПК 2 (Данияр)
27	пр.Тауельсыздык-ул.Куйши Дина-ул.Токпанова
28	пр.Тауелсыздык - ПК 1

29	пр.Тауелсыздык - ул.Майлина
30	пр.Тауелсыздык - ул.Момышулы
31	ул.Токпанова-ул.Момышулы
32	Тауелсыздык - Акыртас
33	пр.Момышулы-ул.Сатпаева
34	пр.Момышулы-СШ№51
35	пр.Момышулы-ул.Жумабаева
36	пр.Абылайхана-пр.Момышулы
37	пр.Момышулы - АстанаЭнергосбыт
38	пр.Момышулы - ул.Кордай
39	Кошкарбаева - Акыртас
40	ул.Жумабаева-ул.Майлина
41	ул.Жумабаева-ул.Куйши Дина
42	ул.Жумабаева-ул.Петрова
43	ул.Жумабаева-ЕНУ
44	ул.Жумабаева-ул.Мунайтпасова
45	ул.Улы Дала-ул.Туркестан
46	ул.Улы Дала-ул.Акмешит
47	ул.Улы Дала-ул.Сауран
48	ул.Рыскулова-ул.Сауран
49	ул.Рыскулова-ул.Акмешит
50	ул.Рыскулова-ул.Туркестан
51	ул.Пушкина-пр.Абая
52	ул.Пушкина-ул.Абылайхана
53	ул.Кудабердыулы-ул.Пушкина
54	пр.Абылайхана- НИИ Травматологии
55	пр.Абылайхана-ул.Жансугурова
56	пр.Абылайхана-ул.Махтумкули
57	пр.Абылайхана-ул.Манаса
58	пр.Абылайхана-Нац Гвардия
59	пр.Абылайхана-ул.Рыскулбекова
60	пр.Абылайхана-ул.Мусрепова
61	пр.Абылайхана- Адиль
62	Джангильдина - ПК 6+80
63	ул.Бейбитшилик-ул.Джангильдина
64	ул.Ауэзова-ул.Джангильдина
65	ул.Бейбитшилик - ул.Сейфуллина
66	ул.Бейбитшилик- пр.Абая
67	Кенесары - Букейхана

68	ул.Ауэзова-ул.Сейфуллина
69	ул.Ауэзова-Омарова
70	ул.Ауэзова- пр.Абая
71	ул.Ауэзова- ул.Кенесары
72	ул.Валиханова- ул.Джангильдина
73	ул.Валиханова- ул.Сейфуллина
74	ул.Валиханова- пр.Абая
75	ул.Валиханова- ул.Кенесары
76	Мангилик Ел - Мед.Центр
77	Мангилик Ел - Кабанбай батыра
78	ул.Косшигулулы-ул.Бейсековой
79	ул.Косшигулулы-ул.Орал
80	Байтурсынова - ПК8+55
81	ул.Кудабердыулы-ул.Жансугурова
82	ул.Кудабердыулы-ПП
83	ул.Кудабердыулы-ул.Манаса
84	ул.Кудабердыулы-ПП
85	ул.Кудабердыулы-ул.Рыскулбекова
86	ул.Кудабердыулы-ул.Мусрепова
87	ул.Кудабердыулы-ул.Мустафина
88	ул.Валиханова- ул.Иманова
89	ул.Желтоксан-пр.Богенбай Батыра
90	ул.Желтоксан-ул.Сейфуллина
91	Акжол-ул.Жанажол
92	Алаш-Военкомат
93	Алаш-ул.69
94	Акжол-ул.Досмухамет улы
95	ул.Сейфуллина-ул.Ракымова
96	ул.Сембинова-ул.Сейфуллина
97	ул.Сембинова-ул.Иманова
98	ул.Иманова-ул.Жубанова
99	ул.Мунайтпасова-ул.Петрова
100	ул.Мунайтпасова-ул.Сатпаева
101	ул.Мунайтпасова-ПК10+30
102	ул. Сатпаева - СШ №48
103	ул.Сатпаева-ул.Петрова
104	ул.Сатпаева-ул.Куйши Дина
105	ул.Сатпаева-ул.Майлина
106	ул.Кудабердыулы - ул.Кошкарбаева

107	ул.Айнаколь-ул.Толебаева
108	ул.Айнаколь-ул.Жумабаева
109	пр.Кошкарбаева- ул.Толебаева
110	пр.Кошкарбаева- ул.Жумабаева
111	ул.Калдаякова-ул.Нажимеденова
112	ул.Калдаякова-ПК41+20
113	ул.Калдаякова-пр.Тауелсыздык
114	ул.Керей Жанибек Хандар- ул.Сауран
115	ул.Керей Жанибек Хандар- ул.Акмешит
116	ул.Керей Жанибек Хандар- ул.Туркестан
117	ул.Керей Жанибек Хандар- ул.Бокейхана
118	ул.Алматы-ул.Сауран

Реконструкция светофорных объектов

№	Наименование перекрестка
1	пр.Тауельсыздык- ул.Мунайтпасова
2	пр.Тауельсыздык- ПК 2
3	пр.Тауельсыздык-ул.Куйши Дина-ул.Токпанова
4	пр.Тауелсыздык - ПК 1
5	пр.Тауелсыздык - ул.Майлина
6	пр.Тауелсыздык - ул.Момышулы
7	пр.Тауелсыздык - ул.Акыртас
8	ул.Токпанова-ул.Момышулы
9	пр.Момышулы-ул.Аманат (СШ51)
10	пр.Абылайхана-пр.Момышулы
11	ул.Айманова-пр.Богенбай Батыра
12	ул.Валиханова- пр.Богенбай Батыра
13	ул.Валиханова- ул.Джангильдина
14	ул.Валиханова- ул.Сейфуллина
15	ул.Валиханова- пр.Абая
16	ул.Валиханова- ул.Кенесары
17	пр.Республики- ул.Сейфуллина
18	ул.Пушкина-пр.Абая
19	ул.Пушкина-ул.Абылайхана
20	пр.Абылайхана-ул.Махтумкули
21	ул.Бейбитшилик - ул.Сейфуллина
22	пр.Республики- ул.Дукенулы
23	пр.Абылайхана-ул.Манаса
24	пр.Абылайхана-Нац Гвардия
25	пр.Абылайхана-ул.Мусрепова
26	пр.Абылайхана- Адиль
27	ул.Бейбитшилик- пр.Абая

28	ул.Кенесары - Букейхана
29	ул.Ауэзова- пр.Абая
30	ул.Ауэзова- ул.Кенесары
31	ул.Сатпаева-ул.КуйшиДина
32	ул.Сатпаева-ул.Майлина
33	ул.Сейфуллина - ул.Ракымова
34	ул.Сейфуллина - ул.Сембинова
35	ул.Кудабердыулы-ул.Пушкина
36	ул.Кудабердыулы-ул.Жансугурова
37	ул.Кудабердыулы-ПП
38	ул.Кудабердыулы-ул.Манаса
39	ул.Кудабердыулы-ПП
40	ул.Кудабердыулы-ул.Рыскулбекова
41	ул.Кудабердыулы-ул.Мусрепова
42	ул.Косшигулулы-ул.Орал
43	пр.Абылайхана-Промышленный
44	пр.Абылайхана-ул.Айнакол
45	ул.Сейфуллина- ул.Айманова
46	пр.Абая-ул.Сембинова
47	пр.Абая-ул.Жубанова
48	ул.Кенесары-ул.Сембинова
49	ул.Кенесары-ул.Бейсекбаева
50	ул.Кенесары-ул.Жубанова
51	ул.Кенесары-ул.Янушкевича
52	ул.Пушкина - ЕНУ
53	пр.Кошкарбаева-ул.Кордай
54	пр.Кошкарбаева-ул.Бесшалкар
55	ул.Мусрепова-ПК1
56	ул.Мусрепова-ПК2
57	ул.Мустафина-ПК1+95
58	ул.Мустафина-ПК4+63
59	пр.Республики-Налоговый Комитет
60	пр.Республики-Есенберлина
61	ул.Гете-ул.Алтын Емел
62	ул.Гете-ул.Алтынсарина
63	Ауэзова-Дукенулы
64	Косшыгулулы-СШ 65 (2)
65	Кудабердыулы - Тойота центр

Остановочные пункты (ОП)

№	Улица	Наименование остановочного пункта
1	ул. Пушкина	Библиотека «Отырар»
2		Библиотека «Отырар»

3	пр. Улы дала	ЖК «Арнау»
4		ЖК «Камал-1»
5		ЖК «Променад ЭКСПО»
6	ул. Кажымукана	Монумент защитников отечества
7		СК «Казахстан»
8		СК «Казахстан»
9		ТД «Орбита»
10		ТД «Орбита»
11		Евразийский национальный университет
12		Евразийский национальный университет
13	ул. Сауран	Ул. Сыганак
14		«ЦОН Есильский»
15	пр. Республики	Микрорайон «Самал»
16		Микрорайон «Самал»
17		Улица Жанибек Тархана
18		Улица А.Иманова
19		Улица А.Иманова
20		Народный банк
21		Народный банк
22		«ЦОН Сарыаркинский»
23		«ЦОН Сарыаркинский»
24		Детская поликлиника №5
25	ул. Валиханова	Ул. Валиханова
26		ТД «Жаннур»
27		ТЦ «Тулпар»
28		Гостиница «Жасыбай»
29		Гостиница «Жасыбай»
30	пр. Кабанбай батыра	Назарбаев Университет
31	пр. Кудайбердыулы	Гостиница «Азамат»
32		Гостиница «Азамат»
33		ЖК «Аламан»
34		ЖК «Аламан»
35		Магазин «Дастан»
36		Магазин «Дастан»
37		Поликлиника №7
38		Поликлиника №7
39		пр. Кудайбердиева
40		Школа-гимназия №52
41		Школа-гимназия №52
42		Гипермаркет «Строймарт»
43	пр. Абылайхана	Пр. Абылайхана

44		Пр. Абылайхана
45		НИИ травмоталогии и ортопедии
46		НИИ травмоталогии и ортопедии
47		Ул. Кажымукана
48		ТД «Гульжан»
49		ТД «Гульжан»
50		Школа «Мирас»
51		Национальный мединский центр
52	ул. Мустафина	Ул. Сілеты
53		Пр. Кудайбердыулы
54	ул. Кенесары	Конгресс-холл
55		Конгресс-холл
56		Пр. Республики
57		Супермаркет «Спутник»
58		Супермаркет «Спутник»
59	ул. Сатпаева	Ул. Сатпаева
60		ТД «Меридиан»
61		ТЦ «Евразия»
62		ТЦ «Евразия»
63		Ул. Майлина
64		Ресторан Туран
65	пр. Момышулы	пр. Тауелсиздик
66		пр. Тауелсиздик
67		Ресторан Туран
68		Ресторан Туран
69		Школа №51
70		Школа №51
71	Ш. Алаш	Рынок «Шарын»
72		Центральный рынок
73	пр. Женис	Театр Жастар
74	ул. Бейбитшилик	Политехнический колледж
75	пр. Кошкарбаева	ЖК «Жайна»
76		ЖК «Турсын Астана»
77	пр. Жумабаева	ЖК «Сарайшык»
78	пр. Тауелсыздык	Монумент защитников отечества
79	ул. Е-10	ЖК «Кулагер»
80		ЖК «Шыгыс»
81		ЖК «Зеленый квартал»
82	ул. Айтматова	ЖК «Меркурий»
83		Ул. Айтматова
84	ул. Сейфуллина	ДС «Бал бала»

85		Школа-гимназия №67
86		Школа-гимназия №65
87		Городская полилкиника № 10
88		Агентство «Хабар»
89		Агентство «Хабар»
90		Гоородская поликлиника № 1
91		Банк «Казком»
92		Банк «Казком»
93		Дворец «Жастар»
94		Дворец «Жастар»
95		Рынок «Астаналык»
96		Рынок «Астаналык»
97	пр. Богенбай батыра	ТЦ «Алем»
98		ТЦ «Алем»
99		ТД «Акжайык»
100		ТД «Акжайык»
101		Ул. Бейбитшилик
102		Ул. Бейбитшилик
103	пр. Тлендиева	Ул. Акан серы
104		Ул. Акан серы
105		Пр. Тлендиева
106		Пр. Тлендиева
107		Рынок «Улжан»
108		Рынок «Улжан»
109		Ул. Сарыбулак
110	ул. Керей-Жанибек хандар	ЖК «Саранда»

Система видеонаблюдения (СВН)

№	Наименование перекрестка
1	пр.Момышулы-ул.Сатпаева
2	пр.Момышулы-ул.Жумабаева
3	пр.Абылайхана-пр.Момышулы
4	пр.Абылайхана-ул.Жансугурова
5	ул.Пушкина-ул.Абылайхана
6	ул.Кудабердыулы-ул.Пушкина
7	ул.Валиханова-ул.Иманова
8	ул.Валиханова- ул.Сейфуллина
9	ул.Валиханова- пр.Богенбай Батыра
10	пр.Республики - "Есиль"
11	пр.Республики- ул.Кенесары

12	пр.Республики-пр. Абая
13	пр.Республики- ул.Сейфуллина
14	пр.Республики- пр.Богенбай Батыра
15	ул.Бейбитшилик- пр.Абая
16	ул.Бейбитшилик- пр.Богенбай Батыра
17	пр.Женис-ул.Есенберлина
18	пр.Тауелсыздык - ул.Момышулы
19	пр.Тауельсыздык-ул.Куйши Дина-ул.Токпанова
20	пр.Тауельсыздык- ул.Мунайтпасова
21	пр.Сарырака-пр.Богенбай Батыра
22	пр.Абылай Хана-ул.Манаса
23	Кургалжинское шоссе-ул.Бейсековой
24	ул.Мунайтпасова-ул.Сатпаева
25	ул.Сатпаева-ул.Петрова
26	пр.Туран-ул.Сарайшик
27	ул.Сарайшик-ул.Туркестан
28	ул.Кунаева-ул.Акмешит
29	ул.Достык-пр.Мангелик Ел
30	пр.Туран-пр.Улы Дала

Источник бесперебойного питания

№	Наименование перекрестка
1	ул.Косшигулулы-ул.Бейсековой
2	пр.Женис-ул.Есенберлина
3	пр.Республики- пр.Богенбай Батыра
4	пр.Республики- ул.Сейфуллина
5	пр.Республики-пр. Абая
6	пр.Республики- ул.Кенесары
7	ул.Валиханова- пр.Богенбай Батыра
8	ул.Валиханова- ул.Сейфуллина
9	ул.Валиханова- пр.Абая
10	ул.Валиханова- ул.Кенесары
11	пр.Тауельсыздык- ул.Мунайтпасова
12	пр.Тауельсыздык-ул.Куйши Дина-ул.Токпанова
13	пр.Тауелсыздык - ул.Момышулы
14	пр.Момышулы-ул.Сатпаева
15	пр.Момышулы-ул.Жумабаева
16	пр.Абылайхана-пр.Момышулы
17	пр.Абылайхана-ул.Жансугурова
18	ул.Пушкина-ул.Абылайхана
19	ул.Кудабердыулы-ул.Пушкина
20	пр. Мангилик Ел - пр. Кабанбай батыра

Система информирования водителей

№	Наименование перекрестка
1	Трасса Каркаралы (Косшы)
2	Трасса Нур-Султан - Караганда
3	Трасса Нур-Султан - Павлодар (Софиевское ш.)
4	Трасса Нур-Султан - Кокшетау (Ондерис)
5	Трасса Нур-Султан - Атбасар (Астраханская)
6	Трасса Нур-Султан - Кургальджино

Магистральные кольца и малые (локальные) кольца ВОЛС, которые вошли в проект:

№	Наименование кольца
1	Магистральное кольцо № 3
2	Магистральное кольцо № 4
3	Малое кольцо №2
4	Малое кольцо №3
5	Малое кольцо №4
6	Малое кольцо №6
7	Малое кольцо №8
8	Малое кольцо №10
9	Малое кольцо №12
10	Малое кольцо №13
11	Малое кольцо №16
12	Малое кольцо №17
13	Резервная серверная ЦУТ (контейнер)

Протяженность прокладки оптоволоконного кабеля 3-й очереди строительства:

№	Наименование кольца	ОК-24	ОК-8
1	Малое кольцо №2	2701	463
2	Малое кольцо №3	0	235,2
3	Малое кольцо №4	5596,8	1884,6
4	Малое кольцо №6	1604,1	559,9
5	Малое кольцо №8	1301,6	778,5
6	Малое кольцо №10	6304,3	354
7	Малое кольцо №12	1887,6	300
8	Малое кольцо №13	7532,9	1496,7
9	Малое кольцо №16	4313,8	1489,5
10	Малое кольцо №17	8104,6	1282,1
11	Магистральное кольцо №3	10208,3	0
12	Магистральное кольцо №4	11881,5	0
13	ЦУТ (контейнер)	1195	0

	Итого	**62631,5**	**8843,5**

Инфраструктура окружающей территории.

Все автоматизируемые перекрестки в рамках проекта ITS оборудованы светофорным оборудованием ITS и дорожными контроллерами. Соединение между контроллером и светофорным оборудованием осуществляется с помощью кабельной канализации, в том числе с использованием канализаций под дорожным полотном, исполненных путем горизонтального бурения грунта (без нарушения дорожного полотна). Светофорные объекты установлены на специализированные металлические консоли, устойчивые к внешним воздействиям окружающей среды (ветер, осадки, перепад сезонных и дневных температур). Светофорные контроллеры установили на бетонном основании в специализированном всепогодном антивандальном шкафу. Все светофорные объекты подключены к городской электрической сети.

Автоматизируемые в рамках проекта ITS остановочные пункты общественного транспорта имеют дорожную инфраструктуру в виде специально выделенного участка дороги (кармана для заезда транспорта), посадочной площадки и специального сооружения для посадки пассажиров, и защиты их от атмосферных осадков.

6.3 Инженерно-технические мероприятия по предупреждению чрезвычайных и взрывопожароопасных ситуаций

Рабочий проект выполнен в соответствии с нормами и правилами в области гражданской обороны, защиты населения и территории от чрезвычайных ситуаций (далее ЧС) природного и техногенного характера.

При подготовке разделов использованы следующие основные руководящие и нормативные документы, действующие в Республике Казахстан: Закон «О чрезвычайных ситуациях природного и техногенного характера» (1996 года с внесенными изменениями и дополнениями от 9 февраля 2009 года), определяющий меры по защите населения, окружающей природной среды и объектов хозяйствования в случае чрезвычайных ситуаций.

На территории строительства отсутствуют взрывоопасные объекты.

В случае чрезвычайных ситуаций ликвидация осуществляется силами ГКП и силами ЧС района.

6.4 Оценка воздействия на окружающую среду

Материалы разработаны: ИП Табигат А. Гладкова-Килкариди, лицензия №02395Р от 23.05.2016 г., выданная Комитетом экологического регулирования, контроля и государтсвенной инспекции в нефтегазовом комплексе Министерства энергетики Республики Казахстан

Заказчик материалов проекта: Государственное учреждение «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур-Султан»

На рассмотрение экологической экспертизы представлены следующие материалы:

- проект «Оценка воздействия на окружающую среду» (II стадия) на 177 страницах;
- Заявление об экологических последствиях, утвержденное Заказчиком намечаемой деятельности;

- Справка о величинах фонового загрязнения в районе расположения площадки намечаемой деятельности, выданная РГП «Казгидромет» №13-09/1905 от 08.06.2020 г.;
- Акт обследования земельного участка на наличие/отсутствие зеленых насаждений, подлежащих сносу/вынужденному переносу №205-7326 от 24.01.2019 г., выданный ГУ «Управление охраны окружающей среды и природопользования г. Астаны»

Материалы поступили на рассмотрение: 06.11.2020 г., входящий номер VE-00056.

Общие сведения

Рабочим проектом предусмотрены работы по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства).

Согласно Санитарных правил «Санитарно-эпидемиологические требования по установлению санитарно-защитной зоны производственных объектов», утвержденных приказом Министра национальной экономики Республики Казахстан №237 от 20.03.2015 г., санитарно-защитная зона на период строительных работ не устанавливается. Согласно статьи 40 Экологического кодекса РК, виды деятельности, не относящие к классам опасности согласно санитарной классификации производственных объектов, классифицируются как объекты IV категории.

Оценка воздействия на атмосферный воздух

На площадке строительства размещается один организованный (ИЗА №0001) и восемь неорганизованных (ИЗА №60001-6008) источников загрязнения атмосферного воздуха. Все источники являются временными и ликвидируются по завершении строительно-монтажных работ.

В атмосферный воздух выделяются ингредиенты восемнадцати наименований, в том числе: первый класс опасности – 1 вещество, второй класс опасности – 3 вещества, третий класс – 9 веществ, четвертый класс – 2 вещества, для двух веществ не определены классы опасности, образуется 1 группа суммации однонаправленного действия (_31).

Расчет загрязнения воздушного бассейна производится по программе расчета приземных концентраций и выпуска томов ПДВ – УПРЗА «ЭРА-2.5». Расчет максимальных приземных концентраций вредных веществ позволяет выделить зоны с нормативным качеством воздуха и повышенным содержанием отдельных ингредиентов по отношению к ПДК. Расчет рассеивания проводился при максимальном режиме работы объекта для всех источников загрязнения с учетом величин фоновых концентраций (справка о величинах фонового загрязнения в районе расположения площадки намечаемой деятельности, выданная РГП «Казгидромет» №13-09/1905 от 08.06.2020 г.).

Анализ результатов расчета показал, что максимальные приземные концентрации по индивидуальным веществам и группам суммаций не оказывают существенного влияния на загрязнение атмосферы, и, следовательно, величина выбросов этих веществ может быть принята в качестве ПДВ. Объект в период строительно-монтажных работ окажет незначительное влияние на атмосферный воздух в районе своего расположения.

Выбросы загрязняющих веществ от передвижных источников загрязнения атмосферного воздуха в соответствие со статьей 28 Экологического кодекса РК при установлении нормативов ПДВ не учитывались.

Обоснованные нормативы выбросов загрязняющих веществ в атмосферу на период строительства приведены в таблице №1.

Таблица 8

Обоснованные нормативы выбросов загрязняющих веществ, выбрасываемых в атмосферу на период строительно-монтажных работ

Производство цех, участок	Номер источника выброса	Нормативы выбросов загрязняющих веществ						
		существующее положение		период строительно-монтажных работ (июль 2021 г.-декабрь 2023 г.)		ПДВ		год достижения ПДВ
		г/с	т/год	г/с	т/год	г/с	т/год	
1	2	3	4	5	6	7	8	9
Организованные источники:								
***(0301) Азота (IV) диоксид (Азота диоксид) (4)								
Площадка строительства	0001	-	-	0.004577778	0.07912	0.004577778	0.07912	2021
***(0304) Азот (II) оксид (Азота оксид) (6)								
Площадка строительства	0001	-	-	0.000743889	0.012857	0.000743889	0.012857	2021
***(0328) Углерод (Сажа, Углерод черный) (583)								
Площадка строительства	0001	-	-	0.000388889	0.0069	0.000388889	0.0069	2021
***(0330) Сера диоксид (Ангидрид сернистый, Сернистый газ, Сера (IV) оксид) (516)								
Площадка строительства	0001	-	-	0.000611111	0.01035	0.000611111	0.01035	2021
***(0337) Углерод оксид (Окись углерода, Угарный газ) (584)								
Площадка строительства	0001	-	-	0.004	0.069	0.004	0.069	2021
***(0703) Бенз/а/пирен (3,4-Бензпирен) (54)								
Площадка строительства	0001	-	-	0.000000007	0.0000001265	0.000000007	0.0000001265	2021
***(1325) Формальдегид (Метаналь) (609)								
Площадка строительства	0001	-	-	0.000083333	0.00138	0.000083333	0.00138	2021
***(2754) Алканы С12-19 /в пересчете на С/ (Углеводороды предельные С12-С19 (в пересчете(10)								
Площадка строительства	0001	-	-	0.002	0.0345	0.002	0.0345	2021
Итого по организованным источникам:		-	-	0.012405007	0.2141071265	0.012321667	0.212727	
Неорганизованные источники								
***(0123) Железо (II, III) оксиды (диЖелезо триоксид, Железа оксид) /в пересчете на(274)								
Площадка строительства	6003	-	-	0.00983	0.000443	0.00983	0.000443	2021
***(0143) Марганец и его соединения /в пересчете на марганца (IV) оксид/ (327)								
Площадка строительства	6003	-	-	0.001137	0.0000512	0.001137	0.0000512	2021
***(0168) Олово оксид /в пересчете на олово/ (Олово (II) оксид) (446)								
Площадка строительства	6003	-	-	0.000001016	0.0000005068	0.000001016	0.0000005068	2021
***(0184) Свинец и его неорганические соединения /в пересчете на свинец/ (513)								
Площадка строительства	6003	-	-	0.00000156	0.000000842	0.00000156	0.000000842	2021
***(0616) Диметилбензол (смесь о-, м-, п- изомеров) (203)								
Площадка строительства	6005	-	-	0.3285	0.0453	0.3285	0.0453	2021
***(2752) Уайт-спирит (1294*)								
Площадка строительства	6005	-	-	0.0137	0.001886	0.0137	0.001886	2021
***(2754) Алканы С12-19 /в пересчете на С/ (Углеводороды предельные С12-С19 (в пересчете(10)								
Площадка строительства	6006	-	-	0.02173	0.581	0.02173	0.581	2021
Площадка строительства	6008	-	-	0.002768232	0.0000015675	0.002768232	0.0000015675	2021
***(2902) Взвешенные частицы (116)								
Площадка строительства	6007	-	-	0.022	0.0198	0.022	0.0198	2021
***(2907) Пыль неорганическая, содержащая двуокись кремния в %: более 70 (Динас) (493)								
Площадка строительства	6001	-	-	0.1778	0.1013	0.1778	0.1013	2021
***(2908) Пыль неорганическая, содержащая двуокись кремния в %: 70-20 (шамот, цемент,(494)								
Площадка строительства	6001	-	-	0.02293	0.026834	0.02293	0.026834	2021
Площадка строительства	6002	-	-	0.0302	0.04745	0.0302	0.04745	2021
***(2930) Пыль абразивная (Корунд белый, Монокорунд) (1027*)								
Площадка строительства	6007	-	-	0.0092	0.00828	0.0092	0.00828	2021
Итого по неорганизованным источникам:		-	-	0.639797808	0.8323471163	0.639797808	0.8323471163	
Всего по предприятию:		-	-	0.652202815	1.0464542428	0.652202815	1.0464542428	

В период эксплуатации нормируемых источников загрязнения атмосферного воздуха нет.

Оценка воздействия на поверхностные и подземные воды

Площадки строительства расположены вне границ водоохранных зон и полос водных объектов. Расстояние до ближайшего водного объекта (р. Есиль) составляет 0.52 км в юго-восточном направлении (участок ул. Кенесары-ул. Янушкевича). Проектируемый объект не предполагает забора воды из поверхностных водных источников и сбросов непосредственно в поверхностные и подземные водные объекты прилегающей территории, поэтому прямого воздействия на водные объекты не оказывает.

Централизованного водоснабжения и канализации на период строительства строительной площадки не предусматривается. В ходе выполнения строительства для обеспечения питьевых нужд персонала водопотребление будет обеспечиваться привозной водой питьевого качества, на технические нужды будет использована вода технического качества. Хранение питьевой воды предусмотрено в специальных резервуарах (емкостях) на строительной площадке и завозится в бутылках.

Сброс хозяйственно-бытовых и производственных стоков на период реконструкции в поверхностные водоемы и на рельеф местности не предусматривается. Хоз-бытовые стоки сбрасываются в биотуалеты с дальнейшим вывозом сторонними подрядными организациями.

Воздействие на водные ресурсы в период строительно-монтажных работ и эксплуатации ожидается незначительное.

Оценка воздействия на почвенный покров

Проектными работами предусмотрено предварительное снятие плодородного слоя почвы на разных участках ведения работ общим объемом 712.0166 тонн глубиной 0.2 метра с последующим складированием под укрытием и последующим использованием при озеленении участков.

При строительно-монтажных работах, учитывая, что работы имеют временный характер, воздействие на почвы прогнозируется непродолжительное и незначительное по воздействию.

В период эксплуатации объекта воздействие на почвы незначительное.

Оценка воздействия на недра

На период строительства и эксплуатации объекта воздействие на недра и геологические структуры не предусматривается.

Оценка воздействия отходов предприятия на окружающую среду

При проведении строительно-монтажных работ будут образовываться отходы производства и потребления зеленого и янтарного уровней опасности.

Таблица 9

Обоснование нормативов образования отходов производства и потребления на период строительно-монтажных работ

Наименование отходов	Образование, т/год	Размещение, т/год	Передача сторонним организациям, т/год

1	2	3	4
Всего	370.92074	-	370.92074
в т.ч. отходов производства	359.321834	-	359.321834
отходов потребления	11.5989	-	11.5989
Янтарный уровень опасности			
Тара из-под ЛКМ (AD060)	0.00084303	-	0.00084303
Зеленый уровень опасности			
Твердые бытовые отходы (GO060)	11.5989	-	11.5989
Мусор строительный (GG170)	350.0	-	350.0
Огарки сварочных электродов (GA090)	0.0004436	-	0.0004436
Красный уровень опасности			
-	-	-	-

Для сбора и временного хранения отходов предусматриваются специальные емкости и площадки. Своевременный сбор, организация временного хранения, утилизация отходов способствуют минимальному воздействию на окружающую среду.

На площадке реконструкции собственные полигоны размещения отходов отсутствуют. Все образующиеся в процессе строительства и эксплуатации отходы будут временно храниться, а затем передаваться по договору специализированным организациям для утилизации и переработки, либо уничтожения.

Воздействие отходов на окружающую среду будет оказываться незначительное.

Оценка воздействия на растительный и животный мир

На территории производства строительных работ редко встречающихся видов растений, занесенных в Красную книгу, не зарегистрировано.

Воздействие на представителей растительного и животного мира в период строительно-монтажных работ носит кратковременный и локальный характер и связано с шумом от строительной техники и механическим воздействием на почвенный покров. Реализация проекта в период эксплуатации не влияет на условия для обитания диких животных и птиц, так как на данной территории отсутствуют пути миграции птиц и скопления крупных животных.

Согласно данных рабочего проекта, на территории рассматриваемого участка проектирования при реализации намечаемой деятельности не предусматривается вырубка и перенос древесных зеленых насаждений (акт обследования земельного участка на наличие/отсутствие зеленых насаждений, подлежащих сносу/вынужденному переносу №205-7326 от 24.01.2019 г., выданный ГУ «Управление охраны окружающей среды и природопользования г. Астаны»).

Отрицательного воздействия на растительный и животный мир не ожидается.

Оценка физических воздействий на окружающую среду

При соблюдении предусмотренных проектных решений при строительно-монтажных работах и эксплуатации объекта вредные факторы физического воздействия на окружающую среду исключаются.

Социально-экономическая среда

Социально-экономическое воздействие данного проекта оценивается как положительное.

Оценка экологического риска намечаемой деятельности

В период строительно-монтажных работ воздействие носит временный характер и не вызывает возникновение и развитие необратимых природных процессов и явлений.

Предлагаемые проектные решения, включающие систему организационно-технических подходов проведения работ и мероприятия по охране окружающей среды, обеспечивают высокую промышленно-экологическую безопасность намечаемого строительства, что делает маловероятным значительные экологические нарушения окружающей среды в районе работ.

В случае возникновения аварийных ситуаций на объекте должно быть обеспечено оперативное оповещение лиц, ответственных за безопасность. Для выяснения причин и устранения последствий аварий должны быть приняты безотлагательные меры.

Вывод

ТОО «VIP Expertiza», рассмотрев рабочий проект «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)» с материалами «Оценка воздействия на окружающую среду» (II стадия) отмечает, что работа выполнена в соответствии с Экологическим Кодексом Республики Казахстан 9 января 2007 года и Инструкции по проведению оценки воздействия на окружающую среду от 28 июня 2007 года № 204-п.

6.5 Организация строительства

Нормативная продолжительность выполнения работ и расчет задела по годам определены в соответствии с СН РК 1.03-01-2016, СП РК 1.03-101-2013, СП РК 1.03-102-2014.

Нормативная продолжительность выполнения работ составляет 28 месяцев.

Начало работ предусмотрено в 3 квартале 2021 года, (письмо ГУ «Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур-Султан» от 25.12.2019 года №503-10-09/2167).

Распределение инвестиций (заделы) по годам строительства:

2021 год – 21,43%

2022 год – 42,86%

2023 год – 35,71%.

6.7 Сметная документация

Сметная документация разработана в соответствии с Нормативным документом по определению сметной стоимости строительства в Республике Казахстан, утвержденным приказом Комитета по делам строительства, жилищно-коммунального хозяйства Министерства по инвестициям и развитию Республики Казахстан от 14 ноября 2017 года № 249-нқ, с изменениями и дополнениями согласно приказа Комитета по делам строительства, жилищно-коммунального хозяйства Министерства индустрии и инфраструктурного развития Республики Казахстан от 11 декабря 2019 года № 205-нқ на основании государственных сметных нормативов, задания на проектирования и принятых проектных решений.

Сметная стоимость строительства, прошедшая экспертизу, подлежит утверждению заказчиком в установленном законодательством порядке и является основанием для определения лимита средств заказчика (инвестора) на реализацию инвестиционных проектов за счет государственных инвестиций в строительство и средств субъектов квазигосударственного сектора в соответствии с пунктом 13 Нормативного документа по определению сметной стоимости строительства в Республике Казахстан.

Сметная документация составлена ресурсным методом с использованием программного комплекса АВС-4 (редакция 2020.4) по выпуску сметной документации в текущих ценах 2020 года.

При составлении смет использованы:

сборники элементных сметных норм расхода ресурсов на строительные работы, ЭСН РК 8.04-01-2015. Выпуск 17;

сборники элементных сметных норм расхода ресурсов на монтажные работы, ЭСН РК 8.04-02-2015. Выпуск 17*;

сборники элементных сметных норм расхода ресурсов на ремонтно-строительные работы, ЭСН РК 8.05-01-2015. Выпуск 17;

сборники сметных цен в текущем уровне 2020 года на строительные материалы, изделия и конструкции, ССЦ РК 8.04-08-2020. Выпуск 2;

сборник сметных цен в текущем уровне 2020 года на эксплуатацию строительных машин и механизмов, СЦЭМ РК 8.04-11-2019;

сборник сметных цен в текущем уровне 2020 года на перевозку грузов для строительства, СЦПГ РК 8.04-12-2019;

перечень оборудования, материалов и изделий, с приложением прайс-листов, наименования которых с соответствующими параметрами и техническими характеристиками отсутствуют в действующих сборниках цен, в соответствии с принятыми и утвержденными решениями заказчика и в соответствии с пунктами 55, 60 и 61 Нормативного документа по определению сметной стоимости строительства в Республике Казахстан.

В сметной стоимости строительства учтены дополнительные затраты:

накладные расходы, определенные в соответствии с Нормативным документом по определению величины накладных расходов и сметной прибыли в строительстве (приложение 2 к приказу от 14 ноября 2017 года № 249-нқ, с изменениями и дополнениями согласно приказа от 14 декабря 2018 года № 257- нқ);

сметная прибыль в размере 8 % от суммы прямых затрат и накладных расходов в соответствии с Нормативным документом по определению величины накладных расходов и сметной прибыли в строительстве (п. 16 приложения 2 к приказу от 14 ноября 2017 года № 249-нқ, с изменениями и дополнениями согласно приказа от 14 декабря 2018 года № 257- нқ);

средства на непредвиденные работы и затраты в размере 2 % от стоимости строительно-монтажных работ по главам 1-9 сметного расчета стоимости строительства (п. 72 приложения 1 к приказу от 14 ноября 2017 года № 249-нқ, с изменениями и дополнениями согласно приказа от 14 декабря 2018 года № 257- нқ);

средства на временные здания и сооружения согласно НДЗ РК 8.04-05-2015;

дополнительные затраты при производстве строительно-монтажных работ в зимнее время НДЗ РК 8.04-06-2015.

Сметная стоимость строительства определена в текущих и прогнозных ценах 2020-2023 годов с учетом текущего и прогнозного уровня инфляции согласно протокола РБК Республики Казахстан от 25 августа 2020 года №29 «Прогноза социально-экономического развития Республики Казахстан на 2021-2025 годы (2020 год -2778 тенге, 2021 год – 2917 тенге, 2022 год – 3063 тенге, 2023 год -3201 тенге).

Налог на добавленную стоимость (НДС) принят в размере, устанавливаемом законодательством Республики Казахстан на период соответствующий периоду строительства, от сметной стоимости строительства.

7. РЕЗУЛЬТАТЫ ЭКСПЕРТИЗЫ

7.1 Дополнения и изменения, внесенные в проект (рабочий проект) в процессе экспертизы:

В процессе рассмотрения по замечаниям и предложениям ТОО «VIP Expertiza» в рабочий проект «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)» внесены следующие изменения и дополнения:

Конструктивные решения

1. Представлено техническое задание и программа выполнения инженерных изысканий в соответствии с п. 5.7, СП РК 1.02-105-2014.
2. Выполнен расчет глубины заложения фундаментов светофорной стойки.
3. Выполнен расчет ветровой нагрузки на светофорные стойки и их фундаменты.
4. Объединены отдельные листы общих данных и конструкций в альбом.
5. Откорректированы ссылки на нормативные документы в соответствие с АГСК-2020.
6. Приведены для чертежей фундаментов марки бетона по водонепроницаемости и морозостойкости.

Наружные сети связи

7. Предоставлено согласование проекта с Заказчиком.
8. Подписали обложку и добавили печать.
9. Добавлены основные показатели проекта в альбомах.
10. Выполнено описание предусмотренных работ в альбомах.
11. Нумерацию листов выполнили согласно ведомости рабочих чертежей.
12. В ПЗ указаны ссылки на действующую нормативно-техническую документацию (НТД) РК согласно АГСК-2020 г.
13. Магистральное кольцо №3, №4. Планы выполнен по существующей трассе. Предоставили согласование.
14. На планах добавили блокировку листов.
15. На планах добавили разрезы.
16. В угловых штампах проектов указаны отсутствующие подписи согласно ГОСТ 21.101-97 «Система проектной документации для строительства.

Оценка воздействия на окружающую среду

17. Представлены ситуационные карты ведения строительных работ;
18. В таблице нормативов эмиссий в атмосферный воздух 2.9.1 уточнен период строительно-монтажных работ в соответствии с письмом Заказчика намечаемой деятельности;
19. Уточнено расстояние до близлежащего водного объекта;

20. В проекте уточнена информация об отсутствии сноса зеленых насаждений; представлен акт обследования земельного участка на наличие/отсутствие зеленых насаждений, подлежащих сносу/вынужденному переносу №205-7326 от 24.01.2019 г., выданный ГУ «Управление охраны окружающей среды и природопользования г. Астаны»;

21. Расчет валовых и максимально-разовых выбросов загрязняющих веществ от источников сыпучих инертных материалов проведен с использованием данных о насыпной плотности материалов;

22. Расчет рассеивания проведен с учетом фонового загрязнения по данным РГП на ПХВ «Казгидромет»;

23. Расчетная часть проекта ОВОС приведена в соответствие с измененной ресурсной сметой рабочего проекта;

24. Материалы заявки на эмиссии в окружающую среду откорректированы.

Сметная документация

25. Оформление и состав сметной документации выполнены согласно указаниям «Государственный норматив по определению сметной стоимости строительства в Республике Казахстан», Приложение 1 к приказу Комитета по делам строительства, жилищно-коммунального хозяйства Министерства по инвестициям и развитию Республики Казахстан от 14 ноября 2017 года № 249-нқ с изменениями и дополнениями согласно приказа Комитета по делам строительства, жилищно-коммунального хозяйства Министерства индустрии и инфраструктурного развития Республики Казахстан от 11 декабря 2019 года № 205-нқ.

26. Выполнена корректировка принятых сметных норм и цен, расхода ресурсов.

27. Объемы приведены в соответствие с откорректированным рабочим проектом.

7.2 Оценка принятых решений

В соответствии с п. 9 раздела 2 приказа Министерства национальной экономики Республики Казахстан от 28 февраля 2015 года № 165 «Об утверждении Правил определения общего порядка отнесения зданий и сооружений к технически и (или) технологически сложным объектам», разработчиком рабочего проекта установлен уровень ответственности объекта – II (нормальный) уровень ответственности, не относящиеся к технически сложным.

Рабочий проект «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)» разработан в необходимом объеме и в соответствии с заданием на проектирование, а также нормативными требованиями.

Состав и комплектность представленных материалов соответствуют требованиям СН РК 1.02-03-2011 «Порядок разработки, согласования, утверждения и состав проектной документации на строительство».

При разработке рабочего проекта учтены местные природно-климатические условия площадки строительства.

В рабочем проекте, согласно имеющимся возможностям, применены импортозаменяющие местные строительные материалы и изделия, изготавливаемые на предприятиях Республики Казахстан.

Принятые проектные решения, с учетом внесенных изменений по п. 7.1 соответствуют государственным нормативным требованиям и функциональному назначению объекта.

Таблица 10

Технико-экономические показатели объекта

№ п/п	Наименование показателя	Ед. изм.	Показатели	
			до рассмотрения	после рассмотрения
1	2	3	4	5
1	Общая сметная стоимость строительства в текущих и прогнозных ценах 2019-2023 годов, в том числе: СМР; оборудование прочие	млн. тенге	11051,685 1804,659 7612,779 1634,247	11103,124 1748,333 7726,859 1627,932
2	Из них: на 2019 год (ПИР) на 2020 год (экспертиза) на 2021 год на 2022 год на 2023 год	млн. тенге		90,878 3,157 2244,012 4677,837 4087,240
3	Нормативная продолжительность выполнения работ	мес	33	28

Примечание: увеличение сметной стоимости строительства в текущих и прогнозных ценах составило 51,439 млн. тенге.

8. ВЫВОДЫ

С учетом внесенных изменений и дополнений рабочий проект «Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)» соответствует требованиям нормативных правовых актов и государственных нормативов, действующих в Республике Казахстан, и рекомендуется для утверждения со следующими основными техническими показателями:

общая сметная стоимость строительства
в текущих и прогнозных ценах 2019-2023 годов - 11103,124 млн. тенге;
в том числе СМР - 1748,333 млн. тенге;
оборудование - 7726,859 млн. тенге;
прочие - 1627,932 млн. тенге;
нормативная продолжительность строительства - 28 месяцев.

Заказчику до начала реализации рабочего проекта получить необходимые согласования и заключения контрольно-надзорных органов и заинтересованных организаций.

Заказчику, при строительстве, максимально использовать оборудование, материалы и конструкции отечественных товаропроизводителей.

Заказчик, при приеме документации по проекту от проектной организации, должен проверить ее на соответствие настоящему экспертному заключению.

8. ТҰЖЫРЫМДАР

Енгізілген өзгерістерді ескере отырып, жобаланатын «Астана қаласының Зияткерлік көлік жүйесін кеңейту бойынша жобалау-сметалық құжаттаманы әзірлеу (құрылыстың 3-ші кезегі)» жұмыс жобасы Қазақстан Республикасында қолданылатын мемлекеттік нормативтердің талаптарына сәйкес келеді және белгіленген тәртіпте келесі негізгі техникалық көрсеткіштерімен бекітілуге ұсынылады:

2019-2023 жылдар ағымдағы және болжам бағалардағы

жалпы сметалық құны	- 11103,124 млн. теңге;
соның ішінде ҚЖЖ	- 1748,333 млн. теңге;
жабдық	- 7726,859 млн. теңге;
басқада шығындар	- 1627,932 млн. теңге;
құрылыстың нормативтік ұзақтығы, барлығы	- 28 ай.

Тапсырысшы жұмыс жобасын іске асыру басталғанға дейін бақылау қадағалау органдары мен мүдделі ұйымдарының қажетті келісімдері мен қорытындыларын алсын.

Тапсырысшы жобалау ұйымынан жұмыс жобасының құжаттамаларын қабылдаған кезде оның осы сараптамалық қорытындыға сәйкестігін тексеруі тиіс.

Тапсырысшы құрылыс кезінде отандық тауар өндірушілердің жабдықтарын, материалдары мен құрылымдарын барынша мол пайдалансын.

Шойымбекова А.С.

Директор

ТОО «VIP Expertiza»

Баукова И.Н.

Эксперт

ТОО «VIP Expertiza»

Цуканова Э.Ф.

Эксперт

ТОО «VIP Expertiza»

Баймашева Ш.М.

Эксперт

ТОО «VIP Expertiza»

Сулейменова А.Т.

Эксперт

ТОО «VIP Expertiza»

Нұрмұхамед А.Н.

Эксперт

ТОО «VIP Expertiza»

Ссылка на окончательную редакцию ПСД

Номер: KZ32VDD00156748

Акимат города Нур-Султан

Государственное учреждение "Управление охраны окружающей среды и природопользования города Нур-Султан"

РАЗРЕШЕНИЕ

на эмиссии в окружающую среду для объектов IV категории

Наименование природопользователя:

Государственное учреждение "Управление транспорта и развития дорожно-транспортной инфраструктуры города Нур -Султан" Республика Казахстан, г.Нур-Султан, район "Сарыарка", улица Бейбітшілік, дом № 11

(индекс, почтовый адрес)

Индивидуальный идентификационный номер/бизнес-идентификационный номер: 151140001473

Наименование производственного объекта: Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)

Местонахождение производственного объекта:

г.Нур-Султан, район "Сарыарка" Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)

Соблюдать следующие условия природопользования:

1. Не превышать лимиты эмиссий (выбросы, сбросы, отходы, сера), установленные в настоящем Разрешении на эмиссии в окружающую среду для объектов IV категории (далее - Разрешение для объектов IV категории) на основании нормативов эмиссий в окружающую среду, установленные и обоснованные расчетным или инструментальным путем и(или) положительными заключениями государственной экологической экспертизы нормативов эмиссий по ингредиентам (веществам) на проекты нормативов эмиссий в окружающую среду, материалы оценки воздействия в окружающую среду, проекты реконструкции или вновь строящихся объектов предприятий согласно приложению 1 к настоящему Разрешению для объектов IV категории.
2. Условия природопользования согласно приложению 2 к настоящему Разрешению для объектов IV категории.
Примечание:
* Лимиты эмиссий, установленные в настоящем Разрешении для объектов IV категории, по валовым объемам эмиссий и ингредиентам (веществам) действуют на период настоящего Разрешения для объектов IV категории и расчитываются по формуле, указанной в пункте 22 Правил заполнения форм документов для выдачи разрешений на эмиссии в окружающую среду.
Разрешение для объектов IV категории действительно до изменения применямых технологий и условий природопользования, указанных в настоящем Разрешении для объектов IV категории.
Приложения 1 и 2 являются неотъемлемой частью настоящего Разрешения для объектов IV категории.

Бегимбеков Айдын Куатжанович

(подпись) Фамилия, имя, отчество (отчество при наличии)

Место выдачи: район "Сарыарка "

Дата выдачи: 21.12.2020 г.

Приложение № 1 к разрешению на эмиссии в окружающую среду

Лимиты эмиссий в окружающую среду

Наименование загрязняющих веществ	Лимиты эмиссий в окружающую среду	
	г/сек	т/год
1	2	3
Лимиты выбросов загрязняющих веществ		
Всего, из них по площадкам:	0,65220281472	1,0464542428
Разработка проектно-сметной документации по расширению Интеллектуальной транспортной системы города Астаны (3-я очередь строительства)	0,65220281472	1,0464542428
в т.ч. по ингредиентам:		
Пыль неорганическая, содержащая двуокись кремния в %:70-20 (шамот, цемент, пыль, цементного производства - глина, глинистый сланец доменный шлак, песок, клинкер, зола кремнезем, зола углей казахстанских месторождений)	0,05313	0,074284
Свинец и его неорганические соединения (в пересчете на свинец)	0,00000156	0,000000842
Пыль абразивная	0,0092	0,00828
Пыль неорганическая, содержащая двуокись кремния в %: более 70 (динас)	0,1778	0,1013
Сера диоксид	0,0006111111	0,01035
Углерод оксид	0,004	0,069
Формальдегид	0,0000833333	0,00138
Уайт-спирит	0,0137	0,001886
Углерод	0,0003888889	0,0069
Алканы С12-19/в пересчете на С/	0,026498232	0,6155015675
Бенз/а/пирен	0,00000000722	0,0000001265
Азот (II) оксид	0,0007438889	0,012857
Азота (IV) диоксид	0,0045777778	0,07912
Взвешенные вещества	0,022	0,0198
Марганец и его соединения (в пересчете на марганец (IV) оксид)	0,001137	0,0000512
Олово оксид (в пересчете на олово)	0,0000010155	0,0000005068
Диметилбензол (смесь о-,м-, п- изомеров)	0,3285	0,0453
Железо (II, III) оксиды	0,00983	0,000443
Лимиты сбросов загрязняющих веществ		
Лимиты на размещение отходов производства и потребления		
Лимиты на размещение серы		

Приложение № 2 к разрешению
на эмиссии в окружающую среду

Условия природопользования

1. Не превышать выбросов загрязняющих веществ в атмосферу установленных настоящим разрешением на эмиссии в окружающую среду.
2. Выбросы загрязняющих веществ в атмосферу исчислять расчетным путем согласно проекту нормативов или проекту оценки воздействия на окружающую среду, по возможности использовать результаты инструментальных замеров по методикам, поквартально.
3. Представлять отчетность, относящуюся к охране природы по форме 870.00- Декларация по плате за эмиссии в окружающую среду с приложениями по форме 870.01.
4. Платежи за загрязнение окружающей среды исчислять по ставкам платы, установленным Решением Маслихата города Нур-Султан. Суммы платы исчислять исходя из фактических объемов загрязнения окружающей среды и установленных ставок. Внесение платы осуществлять в Управление государственных доходов по району Сарыарка г. Нур-Султан.
5. Ежеквартально - в течение 10 рабочих дней после отчетного квартала предоставить отчетность по результатам производственного экологического контроля, согласно приказу Министра энергетики РК «Об утверждении Правил ведения автоматизированного мониторинга эмиссий в окружающую среду при проведении производственного экологического контроля и требований к отчетности по результатам производственного экологического контроля» от 7 сентября 2018 года № 356.
6. Ежеквартально предоставлять отчетность о выполнении условий природопользования.
7. Нарушение экологического законодательства, не исполнение условий природопользования влечет за собой приостановление, аннулирование данного разрешения согласно действующего законодательства.