

**УТВЕРЖДАЮ**  
**АКБ «УЗАГРОЭКСПОРТБАНК»**

**Заместитель  
Председателя Правления**



2022 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Услуги по активации подписок на обновление сервисов информационной безопасности и продление технической поддержки для комплекса сетевой защиты информации, а также, активация программного обеспечения для резервного копирования, репликации и восстановления данных.**

Содержание:

ТЕХНИЧЕСКОЕ ЗАДАНИЕ .....	1
Содержание: .....	2
1. Описание услуги .....	3
2. Цель приобретения услуг .....	3
3. Основание для реализации проекта, в рамках которого производится закупка .....	3
4. Источник финансирования .....	3
4. Спецификация приобретаемой услуги .....	3
5. Спецификация приобретаемой услуги .....	3
5.1 Перечень сервисов .....	3
5.2 Состав услуг по активации подписок на обновление сервисов безопасности .....	3
5.3 Состав услуг, по активации подписок для резервного копирования данных .....	4
6. Требования к услугам по активации .....	6
7. Требования к информационной безопасности .....	6
8. Передоваемая вместе с товарами/услугами документация .....	6
9. Требования к поставщикам услуг .....	7

## 1. Описание услуги

Обновление подписок, должно проходить с использованием программного обеспечения мировых производителей (далее – Система) с официальной гарантией на территории Республики Узбекистан, предназначенное для расширения и внедрения программного комплекса информационной безопасности и системы резервного копирования, репликации и восстановления данных для нужд АКБ «УзАгроЭкспортБанк» (далее – Заказчик).

Потенциальная компания-поставщик (далее: «Поставщик») обязуется предоставить весь необходимый перечень программного обеспечения и сервисов, произвести все необходимые пуско-наладочные работы, связанные с внедрением таких сервисов, поставляемых в рамках услуг настоящего технического задания.

Оказание услуг по активации подписок, на обновление сервисов безопасности и продление технической поддержки, для комплекса информационной безопасности компании Fortinet, Inc, сроком на 1 год», а также, активация подписки на аналогичный срок, на обновление сервисов системы резервного копирования, репликации и восстановления данных Заказчика.

## 2. Цель приобретения услуг.

Обеспечение необходимого уровня сетевой безопасности, и, архивации данных Заказчика.

## 3. Основание для реализации проекта, в рамках которого производится закупка.

Текущие производственные потребности Заказчика.

## 4. Источник финансирования.

Собственные денежные средства Заказчика.

## 5. Спецификация приобретаемой услуги.

### 5.1 Перечень обновляемых сервисов.

В состав комплекса сетевой защиты информации Заказчика, входят следующие продукты компании Fortinet, Inc.:

№	Наименование	Кол-во
1	Межсетевой экран нового поколения (NGFW) Fortigate-201E Network Security Appliance	2
2	Система централизованного хранения событий аудита FortiAnalyzer-200F	1

Перечисленное оборудование установлено в головном офисе Заказчика, в городе Ташкент.

### 5.2 Состав услуг по активации подписок на обновление сервисов безопасности.

Услуги по активации подписок на сервисы безопасности (Unified Threat Protection (UTP)) и продление технической поддержки (FortiCare Contract) оборудования Fortigate-201E и FortiAnalyzer-200F, должны содержать в себе следующие позиции:

№	Код продукта (SKU)	Описание продукта	Кол-во
1	FC-10-00208-950-02-12	FortiGate-201E 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 FortiCare)	2
2	FC-10-L200F-247-02-12	FortiAnalyzer-200F 1 Year 24x7 FortiCare Contract	1

### 5.3 Требования к системе резервного копирования, репликации и восстановления данных.

1	Общие требования к ПО резервного копирования	ПО приобретается в модели на хост по процессорам для резервного копирования виртуальной инфраструктуры на базе VMware vSphere / Microsoft Hyper-V – 1.
2	Поддержка виртуальных инфраструктур	Поддержка резервного копирования виртуальной инфраструктуры на базе платформы VMware vSphere 5.5 и выше, включая VMware vSphere 7, иметь сертификацию VMware Ready for vSAN; Поддержка копирования виртуальной инфраструктуры на базе платформы Microsoft Hyper-V начиная с версии Windows Server 2008 R2 SP1 и выше, включая Microsoft Hyper-V 2019 и поддержку 64 TB VHDX; Поддержка резервного копирования виртуальной инфраструктуры на базе платформы Nutanix AHV с Nutanix AOS 5.1.1 и выше; Поддержка резервного копирования контейнеров vApp, VM и их метаданных, а также их восстановления непосредственно в инфраструктуру vCloud Director. Поддержка автоматизации задачи и обеспечение возможности работы через портал самообслуживания для VMware vCloud Director
4	Общие функциональные возможности платформы резервного копирования	Платформа резервного копирования должна иметь распределенную и горизонтально масштабируемую архитектуру резервного копирования; Платформа резервного копирования должна иметь возможность встроенного резервного копирования самой себя для восстановления настроек; Предоставлять Rest API для удаленного конфигурирования и управления; Обеспечивать использование центрального сервера управления в качестве сервера распределения лицензий;
5	Резервное копирование виртуальных машин	Платформа резервного копирования должна обеспечивать возможность резервного копирования VM на уровне образов, с возможностью копирования только изменившихся блоков и с сохранением состояния приложений, а также без установки специализированных приложений внутрь VM; Платформа резервного копирования должна поддерживать передачу резервных копий, как по сети передачи, так и по сети хранения данных, включая резервное копирование VM напрямую с NFS хранилищ; Платформа резервного копирования должна поддерживать механизм автоматического изменения скорости процесса резервного копирования при увеличении времени отклика на чтение на всех системах хранения с возможностью определения порогов времени отклика; Платформа резервного копирования должна иметь механизм дедупликации и сжатия резервных копий “на лету”, возможность исключать блоки служебных файлов ОС, а также папки и файлы, указанные пользователем, для ускорения процесса резервного копирования, а также для уменьшения объема хранимых данных; Платформа резервного копирования должна уметь использовать аппаратные снимки СХД для резервного копирования, с возможностью обеспечения целостности приложений внутри виртуальных машин. Взаимодействие должно реализовываться при помощи специализированных API на уровне хранилища и без установки дополнительного программного обеспечения на них;
6	Тестирование целостности и возможности восстановления резервных копий виртуальных машин	Платформа резервного копирования должна иметь возможность создать изолированную среду на продуктивной инфраструктуре Заказчика, с возможностью использовать ее для автоматического тестирования резервных копий или для создания тестовых зон; Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности резервных копий VM. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из резервных копий в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри резервируемой VM. Должна быть возможность использовать, как встроенные скрипты проверки, так и возможность использовать собственные скрипты;
9	Хранение резервных копий виртуальных машин	Платформа резервного копирования должна интегрироваться со специализированными решениями для хранения резервных копий (дедуплицирующие устройства дискового хранения): EMC DataDomain по протоколу DDBoost, HPE StoreOnce по протоколу Catalyst, а также Quantum DX, ExaGrid и Fujitsu; Платформа резервного копирования должна иметь возможность шифровать резервные копии; Платформа резервного копирования должна иметь возможность объединения различных физических СХД в логически единый масштабируемый пул хранения резервных копий, для объединения доступного пространства отдельных СХД; Платформа резервного копирования должна иметь возможность перемещения резервных копий на устройства или сервисы объектного хранения на основе протокола S3/S3-совместимый/Azure Blob. Перемещение данных должно производиться, как по достижению определённого времени хранения, так и дублированием данных; Платформа резервного копирования должна уметь передавать резервные копии между различными хранилищами с возможностью указания новой глубины хранения для резервной копии; При передаче резервных копий между хранилищами, платформа резервного копирования должна иметь возможность возобновляемой передачи резервных копий между площадками с использованием механизмов сжатия и глобальной дедупликации трафика, и кэширования информации на обеих площадках на специализированных серверах; Платформа резервного копирования должна поддерживать резервное копирование на ленточные библиотеки, включая многопоточную запись, возможность объединять ленточные накопители в пул с разных ленточных библиотек; Платформа резервного копирования должна иметь возможность формирования синтетической полной резервной копии при записи на ленту из имеющихся в дисковом хранилище резервных копий полной резервной копии и цепочки инкрементальных без создания временной синтетической полной копии на диске;

11	Функциональные возможности репликации и аварийного восстановления виртуальных машин:	<p>Платформа резервного копирования должна поддерживать прямую репликацию виртуальных машин без использования промежуточных резервных копий, с возможностью обеспечения создания множества точек восстановления и передачи только изменившихся блоков;</p> <p>Платформа должна обеспечить целостность приложений внутри VM при репликации, без установки специализированных приложений внутри VM;</p> <p>При репликации VM между хранилищами, платформа резервного копирования должна иметь возможность возобновляемой передачи реплик между площадками с использованием механизмов сжатия и глобальной дедупликации трафика, и кэширования информации на обеих площадках на специализированных серверах;</p> <p>Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину с возможностью автоматической смены IP адреса;</p> <p>Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину даже при потере сервера резервного копирования;</p>
12	Тестирование целостности и возможности восстановления реплицированных виртуальных машин	<p>Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности реплик VM. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из реплик в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри VM. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты;</p>
13	Восстановление данных из резервных копий виртуальных машин	<p>Платформа резервного копирования должна поддерживать возможность восстановления из резервных копий даже в случае полной потери сервера резервного копирования;</p> <p>Платформа резервного копирования должна поддерживать восстановление виртуальных машин как целиком, так и отдельных виртуальных дисков, и файлов конфигураций. Восстановление должно идти как по сети передачи, так и по сети хранения данных;</p> <p>Платформа резервного копирования должна обеспечивать моментальный запуск виртуальных машин непосредственно из хранилища резервных копий, как для платформы VMware vSphere, так и для платформы Microsoft Hyper-V. С возможностью последующего переноса виртуальной машины на выбранное хранилище данных без прерывания работы. Данная технология должна также поддерживаться и для специализированных дедуплицирующих систем хранения;</p> <p>Позволять осуществлять восстановление из резервной копии напрямую в Microsoft Azure/Amazon EC в виде виртуальной машины;</p> <p>Платформа резервного копирования должна обеспечивать возможность предварительного антивирусного сканирования и проверки резервных копий при восстановлении;</p> <p>Платформа резервного копирования должна обеспечивать возможность до восстановления VM в рабочую инфраструктуру удалить данные из этой VM, не удаляя эти данные из резервной копии;</p> <p>Платформа резервного копирования должна реализовывать гранулярное восстановление данных приложений из резервных копий, в промежуточное и/или исходное месторасположение без установки специализированного агента;</p> <p>Платформа резервного копирования должна реализовывать гранулярное восстановление баз данных Oracle на Windows и Linux (с поддержкой технологии ASM), включая возможность восстановления данных до конкретной транзакции, в промежуточное и/или исходное месторасположение без установки специализированного агента. Решение должно быть сертифицировано по программе Oracle Backup Solutions Program (BSP) <a href="http://www.oracle.com/technetwork/database/availability/bsp-088814.html">http://www.oracle.com/technetwork/database/availability/bsp-088814.html</a>;</p> <p>Платформа резервного копирования должна обеспечивать возможность позволять делегировать пользователям самостоятельно восстанавливать из резервной копии объекты приложений через Web-портал;</p>
14	Общие требования к функциям мониторинга, планирования, отчетности среды виртуализации и платформы резервного копирования.	<p>Поддержка не менее двух платформ виртуализации в области мониторинга и планирования нагрузки;</p> <p>Сбор статистики по производительности с платформы резервного копирования;</p> <p>Возможность установки на стандартную ОС, которая покупается отдельно;</p> <p>Наличие встроенной базы знаний, содержащую исчерпывающие сведения о распространенных проблемах виртуальной инфраструктуры и платформы резервного копирования;</p> <p>Моделирование оповещений при изменении пороговых значений производительности, без применения данных значений;</p> <p>Объединение виртуальных машин, хостов или хранилищ в логические группы по любым заданным специализированным критериям: сервис, отдел, город, центр затрат и пр.;</p>
15	Требования к функциям мониторинга виртуальной инфраструктуры	<p>Мониторинг операций ввода/вывода (по отдельности и суммарно), к каждому хранилищу, от каждой виртуальной машины или хоста виртуализации;</p> <p>Мониторинг задержек по чтению и записи, к каждому хранилищу, от каждой виртуальной машины или хоста виртуализации;</p> <p>Мониторинг состояния оперативной памяти, процессоров и сетевых интерфейсов с учетом специализированных метрик виртуализации;</p>
16	Требования к функциям мониторинга инфраструктуры резервного копирования	<p>Мониторинг производительности компонентов резервного копирования по ЦПУ, ОЗУ, дисковой подсистеме и сети передачи данных;</p> <p>Отображение состояние всех компонентов платформы резервного копирования. Текущее состояние задач на резервное копирование и репликацию;</p>
17	Требования к функциям планирования нагрузки и учета виртуальной инфраструктуры	<p>Оценка наиболее и наименее загруженных хостов, и виртуальных машин;</p> <p>Возможность регулярно получать настраиваемые отчеты о производительности хостов и машин в различных форматах;</p> <p>Прогнозирование загрузки хостов и машин на основе данных за прошлые периоды;</p> <p>Получение отчетов, содержащих информацию об избыточно выделенных виртуальным машинам ресурсах;</p> <p>Предоставление рекомендаций по планированию и расширению виртуальной инфраструктуре на любой заданный период в будущем времени;</p> <p>Подготовка отчета об изменениях, произошедших в виртуальной инфраструктуре за любой период времени;</p> <p>Подготовка отчетов, показывающих изменение нагрузки на серверы в кластере, при выходе из строя одного или нескольких из них. Получение рекомендаций;</p> <p>Моделирование добавления новых виртуальных машин и просчет изменения нагрузки на кластер виртуальной инфраструктуры;</p> <p>Создание схемы зависимостей объектов виртуальной инфраструктуры и выгрузка отчета в формате Visio;</p>

18	Требования к функциям планирования нагрузки и учета платформы резервного копирования	Предоставление отчета о системах, которые есть в резервных копиях, но не включенных в задания на резервное копирование; Возможность отслеживания изменения настроек заданий резервного копирования и репликации; Прогнозирование роста объема резервных копий на основе данных за прошлые периоды; Предоставление отчета о ВМ, которые не соответствуют требованиям по минимальному количеству резервных копий; Возможность отслеживания операций восстановления авторизованными пользователями (пользователь, запустивший восстановление и какие объекты были восстановлены); Предоставление отчета о системах, которые присутствуют в нескольких заданиях;
19	Требования к технической поддержке и подписки на обновления системы резервного копирования	Техническая поддержка 1-го уровня должна осуществляться на русском языке с 8:00 до 18:00 (временная зона пользователя); Техническая поддержка должна включать в себя возможность обновления на новые версии ПО той же редакции; Техническая поддержка должна осуществляться в режиме 24 часа, 7 дней в неделю, 365 дней в году; Срок технической поддержки должен составлять не менее 12 месяцев.

### **Требования к технической поддержке оборудования**

- Поддержка должна удовлетворять уровню Standard Support от производителя оборудования.
- Прием запросов и обеспечение реакции на инциденты должны производиться в режиме 24x7 (24 часа, 7 дней в неделю).
- Прием запросов должен осуществляться по прямой телефонной линии, адресу электронной почты либо через личный кабинет на сайте производителя оборудования.
- Каждое обращение должно фиксироваться в регистрационной базе системы технической поддержки производителя оборудования.
- Количество обращений в службу поддержки не должно ограничиваться.
- Услуги по настройке и вводу в эксплуатацию WAF (web-application firewall)

### **Сроки активации услуг**

Период, на который активируются подписки на обновление сервисов информационной безопасности и системы резервного копирования, репликации и восстановления данных – 12 месяцев. Срок, в течение которого активируются услуги – 10 календарных дней.

### **6. Требования к услугам по активации.**

Исполнитель во взаимодействии с производителем оборудования (компанией Fortinet) выполняет все необходимые действия по активации подписок на обновление сервисов безопасности, программного обеспечения используемого оборудования и доступа к сервисам технической поддержки производителя оборудования.

### **7. Требования к информационной безопасности.**

При оказании услуг должны соблюдаться все требования по информационной безопасности в части формирования резервных копий, обеспечения сохранности и целостности существующих информационных баз и банков данных, с возможностью восстановления из резервных копий данных и всех программных средств, действующих до момента установки нового программного обеспечения.

### **8. Передаваемая вместе с товаром/услугами документация.**

Исполнитель должен предоставить акт выполнения услуг и выставить счета-фактуры за оказанные услуги в соответствии с требованиями и сроками, которые будут указаны в договоре на оказание услуг «Оказание услуг по активации подписок на обновление сервисов информационной безопасности и продление технической поддержки для комплекса сетевой защиты информации, а также, активация программного обеспечения для резервного копирования, репликации и восстановления данных, для нужд АКБ «УзАгроЭкспортБанк»».

### **9. Требования к поставщикам услуг.**

- Поставщик услуг должен предоставить письмо от компании-производителя, что поставляемое подписки в рамках услуг настоящего ТЗ будет иметь официальную гарантию и подлежит обслуживанию технической поддержкой производителя;

- Поставщик услуг должен обладать партнерским статусом у компании-производителя, а также обязан предоставить копию письма об Авторизации производителя (MAF) на поставку данного типа решения, в рамках данного конкурса;

- Поставщик должен иметь успешный опыт поставок и внедрения аналогичного решения;

- В рамках запрошенного бюджета, Поставщик обязуется поставить полностью укомплектованное программное обеспечение, необходимое для максимальной полноты решения поставленных Заказчиком задач.

**Внесено:**

**Начальник отдела ИТ**



**Ельцов П.**

