

**Акционерное общество «Петербургская сбытовая компания» (АО «Петербургская сбытовая компания»)**, именуемое в дальнейшем «Покупатель» или «Заказчик», в лице Белокурова Михаила Ивановича, действующего на основании доверенности № 876/1/2021 от 21.12.2021, с одной стороны и

**Общество с ограниченной ответственностью «Бизнес Коммуникации» (ООО «БизКомм»)**, именуемое в дальнейшем «Поставщик» или «Исполнитель», в лице Заместителя генерального директора Пестунова Александра Владиславовича, действующего на основании доверенности от 18.08.2021 № 27, с другой стороны, совместно именуемые «Стороны», заключили настоящий Договор о нижеследующем:

## 1. Предмет Договора

1.1. В соответствии с Договором Поставщик обязуется передать Покупателю Товар, предоставить Сублицензиату неисключительные права на использование программного обеспечения и выдать простую (неисключительную) лицензию на бумажном носителе, на основании которой (которых) Сублицензиат вправе пользоваться сам и предоставить право использования программным обеспечением своим структурным подразделениям, и/или юридическим лицам и провести работы в порядке и на условиях, предусмотренных настоящим Договором и Приложениями к нему.

1.2. Товар (здесь и далее, термин «Товар» включает в себя все позиции **Приложения № 1 (Спецификация)** к настоящему Договору, если не указано иное) на дату его доставки Покупателю должен быть новым и не использованным ранее, отвечать требованиям законодательства, действующего на территории Российской Федерации.

1.3. Поставщик гарантирует, что Товар на дату его поставки Покупателю не заложен, не находится под арестом и не обременен иным образом правами третьих лиц. Если какие-либо указанные в настоящем пункте гарантии впоследствии оказываются неточными или неверными, Поставщик обязуется возместить Покупателю любые убытки, понесенные Покупателем непосредственно в связи с тем, что Покупатель полагался на такие гарантии.

1.4. Объем обязательств Поставщика включает в себя, без ограничения приведенным перечнем:

- поставку Товара в соответствии с **Приложением № 1 (Спецификация)** к настоящему Договору;
- предоставление неисключительных прав на использование программного обеспечения на условиях **Приложения № 5 (Сублицензионный Договор)** к настоящему Договору;
- доставку Товара в части лицензий и сертификатов технической поддержки средствами факсимильной/электронной связи (на e-mail: khachiyants\_na@pesc.ru) и в части оборудования - до склада Покупателя (адрес: 195009 Санкт-Петербург, ул. Михайлова, д. 11);
- проектирование и внедрение системы защиты информации в соответствии с требованиями, указанными в **Приложении № 2 (Задание на проектирование и внедрение)** к настоящему Договору.

1.5. Покупатель обязуется принять и оплатить Товар на условиях настоящего Договора.

1.6. Конкретные условия поставки, сроки поставки, ассортимент, цена и количество поставляемого Товара определяется в **Приложении № 1 (Спецификация)** и **Приложении № 5 (Сублицензионный Договор)** к настоящему Договору.

1.7. Объем и содержание конкретных работ, оказываемых в рамках настоящего Договора, определяется в **Приложении № 2 (Задание на проектирование и внедрение)** к настоящему Договору.

1.8. Работы проводятся силами и средствами Исполнителя. Исполнитель самостоятельно обеспечивает своих работников (специалистов) необходимыми инструментами, приборами, оборудованием, оснасткой, спецодеждой. Исполнитель несет ответственность за качество используемых при оказании услуг материалов, а также обязан предоставить Заказчику необходимые сертификаты на них (соответствия, санитарно-гигиенический и пр.).

## 2. Сумма Договора и порядок оплаты

2.1. Сумма Договора составляет 67 941 053 (шестьдесят семь миллионов девятьсот сорок одна тысяча пятьдесят три) руб. 20 коп., в том числе НДС 20%, в размере 6 006 842 (шесть миллионов шесть тысяч восемьсот сорок два) руб. 20 коп. (далее – Сумма Договора).

2.2. Сумма Договора устанавливается в рублях Российской Федерации. Оплата по настоящему Договору производится в рублях. Днем оплаты признается дата списания денежных средств с расчетного счета Покупателя.

2.3. Сумма Договора включает в себя стоимость Товара, затраты Поставщика по доставке Товара в адрес Покупателя (до склада Покупателя), все налоги, сборы и пошлины, расходы по погрузке, выгрузке, упаковке, таре, проектированию, внедрению, а также



с осуществлением поставки по настоящему Договору. Сумма Договора является фиксированной и не подлежит изменению в течение срока действия настоящего Договора.

2.4. Расчеты по настоящему Договору осуществляются в следующем порядке:

Оплата по настоящему Договору производится в форме безналичного расчёта путём перечисления денежных средств на банковский счёт Поставщика, указанный в разделе 16 настоящего Договора, в течение 60 (шестидесяти) календарных дней с даты подписания Заказчиком Акта приема-передачи Товара, но не ранее 30 (тридцати) календарных дней, с даты подписания УПД. Для оформления реализации товаров/работ/услуг применяется унифицированная форма документа (УПД), которые Поставщик предоставляет Покупателю.

Счета, не подтвержденные документами, не оплачиваются.

2.5. В случае возникновения претензий Покупателя в отношении качества, комплектности, количества и/или ассортимента поставленного Товара или сопутствующих услуг по проектированию и сопровождению, Покупатель вправе после письменного уведомления Поставщика приостановить исполнение обязательства по оплате на период с момента обнаружения нарушения условий о качестве, комплектности, количестве, составе и/или ассортименте и до момента устранения выявленных нарушений Поставщиком. При этом Покупатель не несет ответственности за задержку оплаты за поставленный Товар.

2.6. Поставщик не позднее 5 (пятого) числа месяца, следующего за отчетным кварталом, направляет в адрес Покупателя, оформленный со своей стороны акт сверки. Покупатель в течение 5 (пяти) календарных дней с момента получения акта сверки, производит сверку расчетов между Сторонами, при необходимости оформляет протокол разногласий и возвращает Поставщику один экземпляр надлежаще оформленного акта.

2.7. Стороны осуществляют обмен всеми документами в рамках исполнения обязательств по настоящему Договору, в том числе при выставлении и получении счетов, УПД с использованием электронного документооборота в соответствии с Приложением № 7 (Соглашение об электронном документообороте).

### **3. Права и обязанности сторон**

**3.1. Заказчик обязуется:**

3.1.1. своевременно по запросу Исполнителя предоставлять имеющуюся у Заказчика информацию, необходимую Исполнителю для выполнения своих обязательств в рамках настоящего Договора;

3.1.2. в соответствии с условиями настоящего Договора принять услуги Исполнителя и оплатить их в полном объеме;

**3.2. Заказчик вправе:**

3.2.1. в любое время осуществлять контроль за ходом оказания Исполнителем услуг в рамках настоящего Договора; при обнаружении нарушений Заказчик вправе приостановить работы и потребовать устранения нарушений и оказания услуг в соответствии с условиями настоящего Договора.

**3.3. Исполнитель обязуется:**

3.3.1. оказывать услуги в полном объеме, на высоком профессиональном уровне, в соответствии с заданием Заказчика;

3.3.2. по требованию Заказчика представлять промежуточные отчеты о ходе оказания услуг по Договору;

3.3.3. по окончании оказания услуг предоставить Заказчику отчетные документы, заключения или иные документы об оказанных услугах с приложением подтверждающих документов;

3.3.4. не передавать третьим лицам любую информацию о Заказчике, ставшую известной Исполнителю при оказании услуг по настоящему Договору, за исключением информации, подлежащей раскрытию третьим лицам по законодательству РФ;

3.3.5. при проведении работ на территории Заказчика соблюдать требования правил внутреннего распорядка, пропускного и внутриобъектового режима, установленных у Заказчика, техники безопасности, пожарной безопасности. Заказчик имеет право требовать замену персонала, нарушающего дисциплину;

3.3.6. во исполнение постановления Правительства РФ от 03.12.2020 № 2013 «О минимальной доле закупок товаров российского происхождения» (далее – Постановление № 2013) Исполнитель обязуется не осуществлять замену товара (товаров), содержащегося (содержащихся) в одном из реестров, предусмотренных пунктом 2 Постановления № 2013<sup>1</sup>, на товар (товары), не содержащийся (не содержащиеся) в таких реестрах;

<sup>1</sup> \* Товара, включенного в реестр промышленной продукции, произведенной на территории Российской Федерации, или в реестр промышленной продукции, произведенной на территории государства - члена Евразийского экономического союза, за исключением Российской Федерации, предусмотренные постановлением Правительства Российской Федерации от 30 апреля 2020 г. № 616 «Об установлении запрета на допуск



3.3.7. во исполнение постановления Правительства РФ от 03.12.2020 № 2013 «О минимальной доле закупок товаров российского происхождения» Исполнитель обязуется заполнить и предоставить Заказчику данные о стране происхождения товара, в том числе поставленного при выполнении закупаемых работ, оказании закупаемых услуг, в соответствии с **Приложением № 6** к настоящему договору в течение 10 рабочих дней с момента поставки товара, в том числе поставляемого при выполнении закупаемых работ, оказании закупаемых услуг.

**3.4. Исполнитель имеет право:**

3.4.1. обращаться к Заказчику за предоставлением информации и материалов, необходимых для оказания услуг. Форма предоставления информации, материалов (указать необходимое) определяется Сторонами в рабочем порядке;

3.4.2. привлекать к исполнению настоящего Договора третьих лиц, не предусмотренных настоящим Договором (соисполнителей), только с письменного согласия Заказчика. В этом случае Исполнитель несет перед Заказчиком ответственность за последствия неисполнения или ненадлежащего исполнения обязательств соисполнителем.

#### **4. Качество и комплектность товара**

4.1. Качество и комплектность поставляемого Товара должны соответствовать требованиям Покупателя, государственным стандартам (техническим регламентам), техническим условиям или другой нормативно - технической документации на русском языке, в том числе, указанной в Спецификации, применительно к каждой позиции Товара.

4.2. Поставщик обязан одновременно с передачей Товара передать Покупателю (грузополучателю) его принадлежности, а также относящиеся к нему документы, оформленные надлежащим образом:

- УПД;
- Комплекты документации.

4.3. Товаросопроводительные документы должны быть оформлены на имя грузополучателя. В случае отсутствия необходимых документов Покупатель (грузополучатель) уведомляет об этом Поставщика. Поставщик обязан в течение 3 (трех) рабочих дней с момента получения данного уведомления представить недостающие документы Покупателю (грузополучателю), что не освобождает Поставщика от ответственности, предусмотренной условиями настоящего Договора за нарушение срока поставки.

4.4. В случае, когда принадлежности или документы, относящиеся к Товару, не переданы Поставщиком в указанный срок или/и не предоставлены с Товаром, Покупатель вправе отказаться от Товара, а Поставщик обязан не позднее 15 (пятнадцати) рабочих дней с даты уведомления его Покупателем об отказе от Товара возместить Покупателю понесенные убытки.

4.5. На Товар устанавливается гарантийный срок, равный 12 (двенадцати) месяцам и исчисляемый с даты подписания Сторонами УПД.

4.6. В случае если при внутритарной приемке Товаров, во время производства работ по монтажу Товара или в течение гарантийного срока в Товаре или любой его части будут обнаружены любые дефекты, повреждения, несоответствия (недостатки), Покупатель обязан в разумный срок направить Поставщику уведомление, в котором указывается, что Поставщик по выбору Покупателя:

- производит за свой счет ремонт Товара;
- производит за свой счет замену Товара;
- возвращает Покупателю стоимость Товара;
- возмещает Покупателю расходы, связанные с устранением недостатков Товара.

4.7. Если ремонт товара производился посредством замены комплектующего изделия (или составной части), на которые установлены свои гарантийные сроки, то гарантийный срок на новое комплектующее изделие (или составную часть) исчисляется заново - со дня выдачи товара по окончании ремонта. В течение гарантийного срока Поставщик гарантирует исправную и полнофункциональную работу Товара в соответствии с техническими требованиями к нему, установленными Договором, и возможность его использования по назначению. В течение гарантийного срока Поставщик обеспечит Покупателя

---

промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд, а также промышленных товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок для нужд обороны страны и безопасности государства» **ИЛИ** в единый реестр российской радиоэлектронной продукции, предусмотренный постановлением Правительства Российской Федерации от 10 июля 2019 г. № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации»



консультациями по использованию и поддержке Товара. Стоимость данной услуги Поставщика включена в стоимость Товара.

4.8. В случае, уклонения Поставщика от устранения выявленных дефектов, Покупатель вправе принять меры по их устранению. В последующем Покупатель без ущерба другим своим правам вправе предъявить Поставщику к оплате стоимость выполненных работ, равную произведенным и документально подтвержденным затратам на устранение дефектов, а Поставщик обязан оплатить вышеуказанную сумму.

## **5. Количество товара и график работ**

5.1. Количество, цена, ассортимент поставляемого Товара и график работ указываются Сторонами в Спецификации (**Приложение № 1** к настоящему Договору).

## **6. Тара, упаковка, маркировка товара**

6.1. Товар, поставляемый по настоящему Договору, должен отгружаться Поставщиком в таре и упаковке, с использованием средств пакетирования, соответствующих характеру поставляемого Товара. При этом упаковка должна обеспечивать полную сохранность Товара от всякого рода повреждений и порчи при его перевозке с учетом возможных перегрузок и длительного хранения.

6.2. В случае если по своему характеру Товар не требует затаривания и (или) упаковки и (или) применения средств пакетирования, Поставщик отгружает его без применения этих средств.

6.3. При необходимости согласование способа затаривания, упаковки и средств пакетирования в случае, если отгружаемый Товар требует затаривания, упаковки, применения средств пакетирования, производится Сторонами в Спецификации на каждый вид Товара.

6.4. Товар, упаковка, тара должны быть надлежащим образом промаркированы. При необходимости в Спецификации указывается содержание, способ и места нанесения маркировки.

6.5. Стоимость тары, упаковки включена в цену Товара. Тара, упаковка возврату не подлежит.

## **7. Сроки, порядок и условия поставки**

7.1. Срок поставки Товара – до 21.04.2022. С согласия Покупателя допускается досрочная поставка Товара.

Поставщик в счет цены Договора должен доставить Товар на склад Покупателя, расположенный по адресу: г. Санкт-Петербург, ул. Михайлова, д. 11.

7.2. Сроки проведения работ определяются в **Приложениях № 1 (Спецификация) и № 2 (Задание на проектирование и внедрение)** к настоящему Договору.

7.3. Поставщик обязан направить в адрес Покупателя средствами факсимильной/электронной связи (на e-mail: khachiyants\_na@pesc.ru) информацию о предполагаемой дате поставки Товара (частей Товара) на склад Покупателя не позднее, чем за 2 (два) рабочих дня(ей) до даты такой поставки.

7.4. Право собственности и риск случайного повреждения, гибели Товара переходит от Поставщика к Покупателю с момента подписания УПД. Поставщик считается исполнившим обязательство по поставке Товара Покупателю с момента, указанного в настоящем пункте.

7.5. Поставщик в течение суток с даты отгрузки Товара, обязан уведомить об этом Покупателя средствами факсимильной/электронной связи.

7.6. В случае неприбытия Товара в пункт назначения в течение 7 (семи) дней с даты уведомления об отгрузке, Поставщик за свой счет принимает меры по его розыску.

7.7. В случае если документы первичной отчетности оформлены не по форме и/или оформлены не полностью (отсутствуют обязательные реквизиты, заполнены не все поля, разделы), либо оформлены с ошибками, либо предоставлены не в полном объеме, то Покупатель вправе вернуть такие документы Поставщику на переоформление, не принимать и не оплачивать поставленные Товары на время переоформления Поставщиком таких документов, что не освобождает Поставщика от ответственности за просрочку срока поставки Товара.

7.8. Поставщик, допустивший недопоставку Товара, обязан восполнить недопоставленное количество в течение десяти дней с момента обнаружения недопоставки.

7.9. Покупатель вправе, уведомив Поставщика, отказаться от принятия Товара, поставка которого просрочена более чем на 14 (четырнадцать) календарных дней.

## **8. Порядок сдачи-приемки товара и работ**

8.1. Приемка Товара осуществляется Покупателем совместно с представителями Поставщика в следующем порядке.

8.2. Внешний осмотр тары и упаковки поставочных партий Товара с целью выявления наружных повреждений и проверки соответствия количества отгруженных и поставленных на склад Покупателя





частей Товара выполняется Покупателем без нарушения целостности тары, упаковки и консервации в течение 1 (одного) рабочего дня с даты начала такой приемки.

8.3. Приемка Товара и работ производится по УПД.

8.4. Поставщик в дату, следующую за датой окончания работ (до 12:00 по московскому времени), обязан передать сканированные копии документов, подтверждающих факт поставки и окончания работ, Покупателю средствами факсимильной/электронной связи по номеру факса/адресу электронной почты, указанному в разделе 16 настоящего Договора. Оригиналы документов, подтверждающих факт поставки (подписанные Поставщиком УПД), должны быть направлены Покупателю не позднее 5 (пяти) календарных дней с даты доставки Товара на склад Покупателя.

8.5. Документы, указанные в пункте 8.4. Договора, должны быть оформлены на имя Покупателя. В случае непредставления необходимых копий документов Покупатель уведомляет об этом Поставщика. Поставщик обязан в течение 2 (двух) календарных дней с момента получения данного уведомления Покупателя, но не позднее 7-го числа месяца, следующего за месяцем, в котором были окончены работы, представить недостающие документы Покупателю, что не освобождает Поставщика от ответственности, предусмотренной в пункте 9.7 настоящего Договора. В случае наличия ошибок и иных неточностей в указанных копиях документов Покупатель уведомляет об этом Поставщика в течение 2 (двух) календарных дней с даты получения от Поставщика копий документов. В таком уведомлении Покупатель должен указать способ устранения ошибок и иных неточностей в указанных документах. Поставщик обязан в течение 2 (двух) календарных дней с момента получения данного уведомления от Покупателя устранить ошибки и иные неточности в таких документах и представить копии таких исправленных документов Покупателю, что не освобождает Поставщика от ответственности, предусмотренной в п. 9.7 настоящего Договора.

8.6. В течение 5 (пяти) календарных дней с даты получения подписанных со стороны Поставщика оригиналов УПД Покупатель направляет Поставщику подписанные со своей стороны экземпляры указанных оригиналов документов, либо предоставляет мотивированный отказ в приемке работ или Товара (частей Товара) с указанием дефектов и недостатков, выявленных в процессе приемки, а также с требованием об устранении Поставщиком указанных дефектов и неточностей в приемлемой для Покупателя форме и сроки.

8.7. Внутритарная приемка Товара будет производиться на объекте (складе) Покупателя с участием представителей Покупателя и, при необходимости, Поставщика, с вскрытием ящиков (упаковки) Товара. Внутритарная приемка производится в течение 5 (пяти) календарных дней с даты получения подписанных со стороны Поставщика оригиналов товарных накладных.

8.8. По результатам проверки внутритарной приемки Сторонами составляются и подписываются акты выявленных дефектов (если таковые будут составлены), в которых указывается:

- дата и место составления акта;
- номер и дата Договора;
- наименование Товара (-ов);
- состояние тары и консервации;
- номера мест, в которых обнаружены недостатки, недостача и/или дефект;
- количество мест всей партии Товара;
- описание обнаруженных дефектов, замечаний, повреждений, дефектов и недостатков с приложением фотографий дефектов (для актов выявленных дефектов).

8.9. Если при проверке Товара представители Покупателя и Поставщика разойдутся во мнении о содержании акта проверки, то любая из Сторон может предъявить Товар независимой экспертной организации на повторную проверку. Свидетельство, выдаваемое этой организацией, будет являться основанием для выставления претензий. Затраты по проведению экспертизы относятся на виновную Сторону.

8.10. В случае невозможности прибытия Поставщика к дате, определяемой в соответствии с п. 7.7. настоящего Договора, на внутритарную приемку Товара Покупатель в одностороннем порядке проведет приемку Товара, составит акт проверки и направит его почтовым сообщением в адрес Поставщика, указанный в разделе 17 настоящего Договора. В случае обнаружения дефектов, замечаний, повреждений и т.д. будет составлен акт выявленных дефектов и также направлен в адрес Поставщика.

## **9. Ответственность по Договору**

9.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством РФ.

9.2. За нарушение сроков окончательных расчетов за поставленные по настоящему Договору Товары Покупатель выплачивает по письменному требованию Поставщика неустойку в размере 0,1 % от просроченной суммы за каждый день просрочки, но не более 5 % от суммы задолженности.



- 9.3. За нарушение промежуточных сроков поставки, ассортимента и количества поставляемого Товара Поставщик выплатит по письменному требованию Покупателя неустойку в размере 0,1 % от цены непоставленного товара за каждый день просрочки, но не более 5 % от цены непоставленного товара.
- 9.4. За нарушение итогового срока поставки Товара, указанного в пункте 8.1. Договора, Поставщик выплатит по письменному требованию Покупателя неустойку в размере 0,1 % от цены непоставленного товара за каждый день просрочки.
- 9.5. Если Поставщик поставил Товар не в полном объеме либо не выполнил требования Покупателя о замене недоброкачественного Товара в установленный срок, Покупатель вправе приобрести непоставленный/качественный Товар у других лиц с отнесением на Поставщика разницы стоимости Товара, а также иных расходов, связанных с нарушением Поставщиком своих обязательств по настоящему Договору.
- 9.6. При несвоевременном представлении Поставщиком товаросопроводительной документации, а также при нарушении условий упаковки или маркировки Товара Поставщик возмещает Покупателю убытки, вызванные указанной задержкой или несоблюдением условий упаковки или маркировки, установленных настоящим Договором.
- 9.7. За нарушение Поставщиком сроков исполнения обязательств по предоставлению документов в соответствии пунктами 2.6, 8.4., 8.5. настоящего Договора Покупатель имеет право потребовать от Поставщика уплаты неустойки в размере 1/360 ставки рефинансирования ЦБ РФ от суммы неисполненного обязательства за каждый день просрочки. Стороны договорились, что в случае нарушения Поставщиком сроков исполнения обязательств по предоставлению документов в соответствии с пунктами 2.6, 8.4., 8.5. настоящего Договора для целей расчета неустойки, указанной в настоящем пункте, суммой неисполненного Поставщиком обязательства считается сумма, которая должна быть указана в счете-фактуре и/или документах, подтверждающих факт поставки.
- 9.8. Независимо от уплаты неустойки Сторона, нарушившая Договор, возмещает другой Стороне причиненные в результате этого убытки. Уплата неустойки и возмещение убытков не освобождает Стороны от полного выполнения Сторонами обязательств по Договору.
- 9.9. В случае возникновения претензий к Поставщику независимо от их характера, со Стороны третьих лиц, Покупатель не несет по ним никакой ответственности.
- 9.10. Стороны пришли к соглашению, что в случае изъятия Товара (предъявления требования об изъятии/предполагающее изъятие) у Покупателя при признании Договора недействительным или расторжения Договора по обстоятельствам, возникшим по вине Поставщика, а также вследствие предъявления претензии третьими лицами к Покупателю, в том числе со стороны предыдущих собственников товара или иных третьих лиц, Поставщик обязуется в сроки, указанные в требовании Покупателя, приобрести Покупателю равнозначный товар или предоставить Покупателю денежные средства для самостоятельного приобретения товара, исходя из стоимости аналогичного товара, действующей на рынке аналогичных товаров на момент расторжения Договора (применения последствий недействительности Договора), а также возместить все понесенные убытки и расходы, связанные с приобретением товара по Договору.
- 9.11. В случае непоставки Товара в связи с любыми действиями любого государственного органа любого государства в отношении объявления эмбарго, санкций и т.д. в связи с поставкой Товара на территорию Российской Федерации Покупатель имеет право расторгнуть в одностороннем внесудебном порядке настоящий Договор и потребовать от Поставщика возврата уплаченного по Договору авансового платежа, а также компенсации понесенных Покупателем убытков.
- 9.12. В случае передачи товара ненадлежащего качества Поставщик должен уплатить Покупателю неустойку в размере 0,1 % от цены Договора за каждый день с даты передачи такого товара до полного устранения недостатков товара (замены товара), но не более 5 % от цены Договора.

## 10. Форс-мажор

- 10.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору, если оно явилось следствием природных явлений, военных действий и прочих обстоятельств непреодолимой силы, включая действия и решения органов государственной власти и органов местного самоуправления, и если эти обстоятельства непосредственно повлияли на исполнение настоящего Договора.
- 10.2. Стороны договорились, что для целей исполнения обязательств по настоящему Договору Стороны не будут считать форс-мажорным обстоятельством любые действия любого государственного органа любого государства в отношении объявления эмбарго, санкций и т.д. в связи с поставкой Товара на территорию Российской Федерации.
- 10.3. Сторона, не исполняющая своих обязательств, вследствие обстоятельств непреодолимой силы, должна в 3 (трех) дневный срок сообщить другой Стороне о возникновении такого обстоятельства.



Связанные с форс-мажором обстоятельства должны быть документально подтверждены Торговой Палатой соответствующей страны.

10.4. Срок исполнения обязательств по настоящему Договору отодвигается соразмерно времени, в течение которого действовали обстоятельства непреодолимой силы, а также последствия, вызванные этими обстоятельствами.

10.5. Если обстоятельства непреодолимой силы или их последствия будут длиться более 3 (трех) месяцев, то Покупатель и Поставщик обсудят, какие меры следует принять для продолжения выполнения условий Договора.

10.6. Если в течение 1 (одного) календарного месяца соглашения, устраивающего Стороны не будет достигнуто, каждая из Сторон вправе потребовать расторжения настоящего Договора.

10.7. Стороны договорились, что для целей исполнения обязательств по настоящему Договору Стороны не будут считать форс-мажорным обстоятельством действия государственных органов РФ (органов субъектов РФ, органов местного самоуправления), связанные с принятием мер государственного реагирования, принятых в связи с распространением коронавирусной инфекции COVID-19, о которых сторонам известно на дату заключения настоящего Договора.

## **11. Заверения об обстоятельствах**

10.1. Поставщик заверяет Покупателя, что на момент заключения Договора и в течение всего времени его действия:

а) работники и иные физические лица, привлекаемые Поставщиком для исполнения обязательств, возникших из настоящего Договора, имеют необходимые для этого знания, опыт и квалификацию, подтверждаемые соответствующими документами.

б) заключение и исполнение настоящего Договора не противоречит и не представляет собой нарушения какого-либо иного обязательства Поставщика, проистекающего из какой-либо сделки или иного основания;

с) Поставщик является платежеспособным и состоятельным. Термины «платежеспособный и состоятельный» для целей настоящего Договора означает:

– что чистые активы Поставщика составляют положительную величину, превышающую размер его уставного капитала;

– Поставщик способен надлежащим образом исполнять свои обязательства по мере того, как такие обязательства становятся обязательными к исполнению;

– Поставщик не имеет намерения принимать на себя обязательства, исполнение которых он не мог бы осуществить надлежащим образом;

– в отношении Поставщика не имеется возбужденного дела о банкротстве, включая процедуру наблюдения, финансового оздоровления, внешнего управления, конкурсного производства;

– Поставщик не располагает сведениями о факте подачи кредитором или намерении кредитора подать в отношении Поставщика заявление о признании его банкротом;

д) Поставщик обладает ресурсами, технологиями, деловыми связями, знаниями, навыками и умениями, а также опытом, необходимыми для исполнения обязательств, возникших из настоящего Договора;

е) Поставщик, а также привлекаемые в целях исполнения настоящего Договора соисполнители являются добросовестными налогоплательщиками.

ф) Поставщик, а также привлекаемые в целях исполнения настоящего Договора соисполнители включили в состав расчета налоговой базы для целей исчисления и уплаты НДС и налога на прибыль хозяйственные операции, совершенные в рамках настоящего договора.

г) в отношении каждого привлекаемого Поставщиком соисполнителя Поставщик запросит и изучит информацию и документы (аналогичные информации и документам, запрошенным Покупателем у Поставщика), достаточные для вывода о том, что порядок исчисления и уплаты налогов таким соисполнителем соответствует требованиям действующего налогового законодательства;

h) Поставщик располагает необходимыми документами, свидетельствующими о том, что порядок исчисления и уплаты налогов таким соисполнителем соответствует требованиям действующего налогового законодательства.

10.2. Стороны подтверждают и соглашаются с тем, что указанные в настоящем Договоре заверения об обстоятельствах, а также заверения об обстоятельствах, которые будут предоставляться в период действия настоящего Договора:

– являются заверениями об обстоятельствах по смыслу ст. 431.2 Гражданского кодекса Российской Федерации, которые имеют значение для заключения и исполнения настоящего Договора;

– составляют сведения, на которые полагается Покупатель при заключении и исполнении настоящего Договора.



## 12. Возмещение имущественных потерь

12.1. В соответствии с нормами ст. 406.1 Гражданского кодекса Российской Федерации Стороны согласовали, что независимо от достоверности или недостоверности заверений об обязательствах, данных Поставщиком в соответствии с настоящим Договором, Поставщик обязуется возместить все имущественные потери Покупателя, возникшие в случае наступления определенных в настоящем Договоре обстоятельств и не связанные с нарушением обязательства Поставщиком.

12.2. Возмещению подлежат потери Покупателя, возникшие в случаях предъявления третьими лицами или органами государственной власти, в том числе органами, осуществляющими государственный (муниципальный) контроль (надзор) (далее – органами государственной власти), требований, жалоб, претензий, исков или начисления каких-либо обязательных к уплате платежей, если они прямо или косвенно вытекают из договора и связаны с действиями и(или) бездействиями Поставщика, соисполнителей, или с их юридическим статусом.

В данном случае под потерями понимаются расходы Покупателя, которые он произвел или должен будет произвести, включая, но не ограничиваясь, уплату налогов, иных обязательных платежей, штрафов, судебных расходов, судебных и внесудебных выплат.

Возмещение потерь допускается, если потери уже понесены или с неизбежностью будут понесены в будущем.

К имущественным потерям Покупателя в том числе относятся суммы недоимки по налогам (налог на прибыль, НДС), соответствующие суммы штрафов, пеней при наличии в совокупности следующих обстоятельств:

- в порядке применения ст. 101 Налогового кодекса Российской Федерации налоговым органом в отношении Покупателя вынесено решение о привлечении к ответственности / отказе в привлечении к ответственности за совершение налогового правонарушения с указанием сумм недоимки по налогам (налог на прибыль, НДС), соответствующих сумм штрафов, пеней, вызванных недобросовестными действиями Поставщика, а также привлеченных в целях исполнения настоящего Договора соисполнителей при исчислении и уплате налогов;

- суммы недоимки по налогам (налог на прибыль, НДС), соответствующие суммы штрафов, пеней будут списаны с банковского счета Покупателя в безакцептном порядке / перечислены Покупателем добровольно по требованию налогового органа.

12.3. Стороны согласовали, что с момента получения от третьих лиц или органов государственной власти требований, жалоб, претензий, исков, а также в порядке статьи 100 Налогового кодекса Российской Федерации акта налоговой проверки, в которых отражены имущественные притязания и/или выявлены нарушения законодательства, вызванные недобросовестными действиями Поставщика в том числе при исчислении и уплате налогов, а также привлеченных в целях исполнения настоящего договора соисполнителей, Покупатель направляет в адрес Поставщика копию требований, жалоб, претензий, исков или выписку из акта налогового органа по соответствующему эпизоду.

12.4. Стороны согласовали, что в случае несогласия с фактами, изложенными в приведенных выше документах, а также с выводами и предложениями проверяющих органов государственной власти, Поставщик в течение 10 (десяти) календарных дней с момента получения документов направляет в адрес Покупателя письменные мотивированные возражения по фактам (выводам проверяющих органов государственной власти), содержащимся в них, которые Покупатель обязан представить в адрес третьего лица или проверяющего органа государственной власти.

В случае непредставления Поставщиком в указанный выше срок письменных мотивированных возражений по фактам (выводам третьих лиц или проверяющих органов государственной власти), содержащимся в представленных документах, Поставщик считается согласившимся с правомочностью выводов третьих лиц и проверяющих органов государственной власти, изложенных в представленных документах, и полностью снявшим с Покупателя обязанность по оспариванию выводов третьих лиц и проверяющих органов государственной власти.

12.5. Поставщик возмещает Покупателю имущественные потери в течение 10 (десяти) дней с даты предъявления Покупателем соответствующего требования путем перечисления денежных средств на расчетный счет Покупателя.

12.6. Потери возмещаются независимо от признания договора незаключенным и(или) недействительным.

12.7. Размер потерь определяется исходя из стоимости требований, предъявленных третьими лицами и(или) органами государственной власти к Покупателю.

12.8. В случае, если потери возникли в связи с неправомерными действиями соисполнителя или иного третьего лица, к Поставщику, возместившему такие потери, переходит требование кредитора к таким лицам о возмещении убытков.





12.9. В случае, если после возмещения Поставщиком имущественных потерь имущественные притязания третьего лица или решение (иной ненормативный акт) органа государственной власти будут признаны незаконными в той части, в соответствии с которой Поставщиком было произведено возмещение имущественных потерь Покупателя, Покупатель обязуется возратить Поставщику полученную сумму (без учета процентов) в размере возвращенных взысканных сумм. При этом проценты, предусмотренные ст. 395 Гражданского кодекса Российской Федерации, не подлежат начислению на сумму, возвращенную Покупателю.

### **13. Разрешение споров**

13.1. Если, в соответствии с требованиями действующего законодательства РФ соблюдение претензионного порядка для обращения в суд является обязательным, то спор, возникающий из правоотношений, связанных с исполнением Сторонами настоящего Договора, может быть передан на разрешение арбитражного суда по истечении 7 (семи) календарных дней со дня направления претензии в адрес Поставщика посредством почтовой связи либо по истечении 5 (пяти) календарных дней со дня направления претензии в адрес Поставщика посредством факсимильной связи либо электронной почты. Такая претензия может быть направлена посредством почтовой, факсимильной связи или по электронной почте в адрес Поставщика по реквизитам, указанным в разделе 16 настоящего Договора. Если в соответствии с требованиями действующего законодательства РФ соблюдение претензионного порядка для обращения в суд не является обязательным, то спор, возникающий из правоотношений, связанных с исполнением Сторонами настоящего Договора, может быть передан на разрешение арбитражного суда без предварительного направления претензии Стороне.

13.2. При невозможности урегулирования споров путем переговоров споры разрешаются в Арбитражном суде города Санкт-Петербурга и Ленинградской области.

### **14. Основания расторжения Договора**

14.1. Покупатель вправе в одностороннем порядке отказаться от исполнения настоящего Договора в следующих случаях:

14.1.1. задержки Поставщиком выполнения обязательств по настоящему Договору более чем на 20 (двадцать) рабочих дней по причинам, не зависящим от Покупателя (в том числе сроков выполнения работ);

14.1.2. нарушения Поставщиком условий настоящего Договора, ведущее к существенному снижению качества Товара (в том числе при поставке некачественного Товара) или ненадлежащему качеству проводимых работ;

14.1.3. в случае непоставки Товара в связи с любыми действиями любого государственного органа любого государства в отношении объявления эмбарго, санкций и т.д. в связи с поставкой Товара на территорию Российской Федерации;

14.1.4. в иных случаях ненадлежащего исполнения обязательств Поставщиком;

14.1.5. при установлении нецелесообразности дальнейшего исполнения Договора, определяемой Покупателем – с возмещением Поставщику фактически понесенных затрат.

14.2. Уведомление о расторжении настоящего Договора должно быть направлено Поставщику посредством факсимильной / электронной связи не позднее, чем за 7 (семь) рабочих дней до предполагаемой даты его расторжения с последующей досылкой на бумажном носителе.

14.3. Договор считается расторгнутым по основаниям, предусмотренным пунктом 14.1. настоящего Договора, с даты, указанной в уведомлении о расторжении настоящего Договора.

14.4. В случае расторжения настоящего Договора, Покупатель вправе потребовать от Поставщика возврата ранее уплаченных сумм, в том числе, причиненных убытков.

### **15. Заключительные положения**

15.1. Вся информация, полученная в ходе реализации настоящего Договора, включая информацию о финансовом положении Сторон, считается конфиденциальной и не подлежит разглашению или передаче третьим лицам, как в период действия настоящего Договора, так и по окончании его действия в течение 5 (пяти) лет.

15.2. При изменении реквизитов, Стороны обязуются извещать друг друга о таких изменениях в 2 (двух) дневной срок. В противном случае сообщения и расчеты, переданные и произведенные по последнему известному адресу и реквизитам, считаются переданными и произведенными надлежащим образом.

15.3. Документы, переданные средствами факсимильной/электронной связи, имеют юридическую силу, оригиналы указанных документов направляются по почте в течение 7 (семи) рабочих дней с даты передачи средствами факсимильной/электронной связи.



15.4. Поставщик не вправе передавать свои права и обязанности по настоящему Договору третьим лицам без письменного согласия Покупателя.

15.5. Поставщик обязуется раскрывать Покупателю сведения о собственниках (номинальных владельцах) акций Поставщика, владеющих не менее чем 5% общего количества размещенных голосующих акций общества, по форме, предусмотренной **Приложением № 3 (Форма по раскрытию информации в отношении всей цепочки собственников, включая бенефициаров (в том числе, конечных))**, с указанием бенефициаров (в том числе конечного выгодоприобретателя/ бенефициара) с предоставлением подтверждающих документов.

В случае изменений сведений о собственниках (номинальных владельцах) акций Поставщика, включая бенефициаров (в том числе конечного выгодоприобретателя/бенефициара), а также о смене единоличного исполнительного органа, Поставщик обязуется в течение 5 (пяти) календарных дней с даты соответствующего изменения предоставить Покупателю актуализированные сведения.

При раскрытии соответствующей информации Стороны обязуются производить обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и передают Покупателю согласия на обработку персональных данных согласно **Приложению № 4 (Форма согласия на обработку персональных данных)**.

Положения настоящего пункта Стороны признают существенным условием Договора. В случае невыполнения или ненадлежащего выполнения Поставщиком обязательств, предусмотренных настоящим пунктом, Покупатель вправе в одностороннем внесудебном порядке расторгнуть Договор.

15.6. Стороны обязуются при передаче информации соблюдать запреты, установленные антимонопольным законодательством, в том числе обязуются не использовать полученную информацию с целью недопущения, ограничения, устранения конкуренции и (или) ущемления интересов других лиц (хозяйствующих субъектов) в сфере предпринимательской деятельности либо неопределенного круга потребителей, в том числе обязуются не совершать действий (бездействия), указанных в статьях 10, 11, 11.1, 14.7 Федерального закона от 26.07.2006 №135-ФЗ «О защите конкуренции».

Стороны подтверждают, что передача информации осуществляется исключительно в целях обмена информацией в рамках потенциальных проектов по купле-продаже

15.7. Настоящий Договор выражает все договорные условия и понимание между Сторонами в отношении всех упомянутых здесь вопросов, при этом все предыдущие обсуждения, обещания, согласования и представления между Сторонами, если таковые имелись, кроме упомянутых в тексте настоящего Договора, теряют силу и заменяются вышеизложенным текстом.

15.8. Настоящий Договор вступает в силу с даты подписания его Сторонами и действует в части поставки и проведения работ до 30.06.2022, в части взаиморасчетов, гарантии, технической поддержки и соблюдения конфиденциальности до полного исполнения обязательств Сторонами.

15.9. Все изменения и дополнения к настоящему Договору должны быть совершены в письменной форме в виде единого документа и вступают в силу после подписания обеими Сторонами.

15.10. В части, не урегулированной настоящим Договором, отношения Сторон регламентируются действующим законодательством Российской Федерации.

15.11. Договор составлен в 2 (двух) подлинных экземплярах, по одному для каждой из Сторон. Оба экземпляра имеют равную юридическую силу.

### 15. Приложения к настоящему Договору

- Приложение № 1 – Спецификация;
- Приложение № 2 – Задание на проектирование и внедрение;
- Приложение № 3 – Форма по раскрытию информации в отношении всей цепочки собственников, включая бенефициаров (в том числе, конечных);
- Приложение № 4 – Форма согласия на обработку персональных данных;
- Приложение № 5 – Сублицензионный договор;
- Приложение № 6 – Форма предоставления информации о стране происхождения товара, в том числе поставляемого при выполнении закупаемых работ, оказании закупаемых услуг.

Все приложения к настоящему Договору являются его неотъемлемой частью.

### 16. Адреса и реквизиты Сторон

<b>Поставщик:</b>	<b>Покупатель:</b>
-------------------	--------------------



<p> <b>ООО «БизКомм»</b>  ИНН 7714856880 КПП 772401001  ОГРН 1117746926593  Юридический адрес: 115230, г. Москва, проезд  Хлебозаводский, д. 7, стр. 9, эт. 3, пом. X, ком. 25,  оф. 14  Почтовый адрес: 119334, г. Москва, а/я 85  ОКПО 37215155  ОКТМО 45918000  e-mail: in@biz-komm.ru  телефон: +7 (495) 900-10-65  Банковские реквизиты:  р/с 40702810747010001406  в ЦЕНТРАЛЬНЫЙ ФИЛИАЛ АБ "РОССИЯ"  к/с 30101810145250000220  БИК 044525220 </p>	<p> <b>АО «Петербургская сбытовая компания»</b>  ИНН 7841322249 КПП 780401001  ОГРН 1057812496818  Юридический адрес: 195009, Санкт-Петербург,  ул. Михайлова, дом 11  Почтовый адрес: 195009, Санкт-Петербург, ул.  Михайлова, дом 11  ОКПО 77724330  ОКТМО 403300000000  e-mail: office@pesc.ru  телефон: +7 (812) 303-69-69  факс: +7 (812) 327-07-03  Банковские реквизиты:  р/с 407028109000000028772  в БАНК ГПБ (АО) г. Москва  БИК 044525823  к/с 30101810200000000823 </p>
<p>Заместитель генерального директора</p> <p>_____ Пестунов А.В.</p>	<p>Директор по информационным технологиям</p> <p>_____ Белокуров М.И.</p>



# Приложение № 1

к Договору поставки № 22-100

от 03.03.2022 г.

## СПЕЦИФИКАЦИЯ

Объект: (наименование объекта): 195009, Санкт-Петербург, ул. Михайлова, дом 11

Грузополучатель: АО «Петербургская сбытовая компания»

Поз. №	Наименование Товара	Кол-во, всего (шт.)	Цена Товара за ед. без НДС (руб.)	Сумма Товара без НДС (руб.)	НДС		Сумма Товара с НДС (руб.)	Наименование производителя	Наименование Страны производителя	Наименование товара от производителя <sup>2</sup>
					Ставка %	Сумма НДС (руб.)				
1	Лицензия (право на использование) на программное обеспечение (ПО) MaxPatrol Security Information and Event Management, компонент MaxPatrol SIEM Agent, для выявления сетевых аномалий (подозрительной активности) в системах управления базами данных, активный сбор не более чем с 1000 узлов, прием не более 3000 событий в секунду. Срок действия лицензии – бессрочно (не более срока действия исключительных прав правообладателя). Гарантийные обязательства (базовая поддержка) в течение 1 года. PT (POSITIVE TECHNOLOGIES) PT-MPSIEM-AGT-R	3	2 900 000,00	8 700 000,00	0	0	8 700 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Права на программы для ЭВМ Программное обеспечение MaxPatrol Security Information and Event Management. Компонент MaxPatrol SIEM Agent, активный сбор не более чем с 1000 узлов, прием не более 3000 событий в секунду, гарантийные обязательства в течение 1 (одного) года PT-MPSIEM-AGT-R (Запись в Реестре №11898 от 22.10.2021)
2	Лицензия (право на использование) на программное обеспечение (ПО) Network Attack Discovery Capturer, для анализа сетевого трафика (NTA) и выявления атак на периметре и внутри сети, до 5000Мбит/с, на 1 пользователя. Срок действия лицензии – бессрочно (не более срока действия исключительных прав правообладателя). Гарантийные обязательства (базовая поддержка) в течение 1 года.	2	5 400 000,00	10 800 000,00	0	0	10 800 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Права на программы для ЭВМ Программное обеспечение Positive Technologies Network Attack Discovery. Компонент Network Attack Discovery Capturer, до 5 000 Мбит/с, гарантийные обязательства в течение 1 (одного) года PT-NAD-CAP-5000 (Запись в Реестре №11897 от 22.10.2021)

<sup>2</sup> Для программного обеспечения добавляются сведения о включении в Единый реестр российских программ для электронных вычислительных машин и баз данных (далее – Реестр)





Поз. №	Наименование Товара	Кол- во, всего (шт.)	Цена Товара за ед. без НДС (руб.)	Сумма Товара без НДС (руб.)	НДС		Сумма Товара с НДС (руб.)	Наименование производителя	Наименование Страны производителя	Наименование товара от производителя <sup>2</sup>
					Ставка %	Сумма НДС (руб.)				
	PT (POSITIVE TECHNOLOGIES) PT-NAD-CAP-5000									
3	Лицензия (право на использование) на программное обеспечение (ПО) Network Attack Discovery Server, для анализа сетевого трафика (NTA) и выявления атак на периметре и внутри сети, на 1 пользователя. Срок действия лицензии – бессрочно (не более срока действия исключительных прав правообладателя). Гарантийные обязательства (базовая поддержка) в течение 1 года. PT (POSITIVE TECHNOLOGIES) PT-NAD-SRV	2	3 600 000,00	7 200 000,00	0	0	7 200 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Права на программы для ЭВМ Программное обеспечение Positive Technologies Network Attack Discovery. Компонент Network Attack Discovery Server, гарантийные обязательства в течение 1 (одного) года PT-NAD-SRV (Запись в Реестре №11897 от 22.10.2021)
4	Лицензия (право на использование) на программное обеспечение (ПО) Network Attack Discovery, для анализа сетевого трафика (NTA) и выявления атак на периметре и внутри сети, базовая на 5Гбит/с, на 1 пользователя. Срок действия лицензии – бессрочно (не более срока действия исключительных прав правообладателя). Гарантийные обязательства (базовая поддержка) в течение 1 года. PT (POSITIVE TECHNOLOGIES) PT-NAD-BASE-5	2	2 600 000,00	5 200 000,00	0	0	5 200 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Права на программы для ЭВМ Программное обеспечение Positive Technologies Network Attack Discovery. Базовая лицензия на 5 Гбит/с, гарантийные обязательства в течение 1 (одного) года PT-NAD-BASE-5 (Запись в Реестре №11897 от 22.10.2021)
5	Сервер ThinkSystem SR530, форм фактор Rack 1U, установка до 2 процессоров, 12 слотов под оперативную память TruDDR4 2666МГц до 768Гб, установка до 8 жестких дисков 2,5" SAS/SATA, сетевой интерфейс 10GbE 2P, установка до 2 блоков питания с горячей заменой, в составе: ThinkSystem SR530 2.5" Chassis with 8 Bays (AV0S), Operating mode selection for: Efficiency - Favoring Performance Mode (BFYE), Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor (B7N6) 2шт, ThinkSystem 16GB	6	1 127 702,00	6 766 212,00	20	1 353 242,40	8 119 454,40	Lenovo	Китай	ThinkSystem SR530, 2xIntel Xeon Silver 4214R 12C 2.4GHz 100W, 4x16GB 2Rx8, 4x1.2TB 10000, RAID 930-16i 8GB Flash PCIe 12Gb Adapter, 2x750W, XCC Enterprise, ThinkSystem Toolless Slide Rail, 7X08SNCS00



Поз. №	Наименование Товара	Кол- во, всего (шт.)	Цена Товара за ед. без НДС (руб.)	Сумма Товара без НДС (руб.)	НДС		Сумма Товара с НДС (руб.)	Наименование производителя	Наименование Страны производителя	Наименование товара от производителя <sup>2</sup>
					Ставка %	Сумма НДС (руб.)				
	TruDDR4 2933MHz (2Rx8 1.2V) RDIMM (B4H2) 4шт, ThinkSystem SR530/SR630/SR570 2.5" SATA/SAS 8-Bay Backplane (AUWB), Select Storage devices - no configured RAID required (5977), ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E), ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD (AUM1) 4шт, ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit (AUWC), ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit (AUWA), Lenovo ThinkSystem 1U LP+LP BF Riser Bracket (AUWQ), ThinkSystem 1Gb 2-port RJ45 LOM (AUKG), T									
6	Сервер ThinkSystem SR590, форм-фактор 2U, в составе: ThinkSystem SR590 3.5" Chassis with 8 or 12 Bays (AXEB), Operating mode selection for: "Efficiency - Favoring Performance Mode" (BFYE), Intel Xeon Gold 6230R 26C 150W 2.1GHz Processor (BAZX) 2шт, ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM (B4H3) 4шт, ThinkSystem 2U 3.5" SATA/SAS 12-Bay Backplane (AUR9), Select Storage devices - no configured RAID required (5977), ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E), ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD (AUU8) 12шт, ThinkSystem M.2 with Mirroring Enablement Kit (AUMV), ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD (B8HS) 2шт, ThinkSystem SR590 x8/x8/x8 PCIe Riser 1 (B261), ThinkSystem 10Gb 2-port SFP+ LOM (AUKJ), ThinkSystem Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter (AUKX), ThinkSystem 750W(230/115V)	2	1 894 835,00	3 789 670,00	20	757 934,00	4 547 604,00	Lenovo	Китай	ThinkSystem SR590, 2xIntel Xeon Gold 6230R 26C 2.1GHz 150W, 4x32GB 2Rx4, 240GBx2 SATA, 12x4TB 7200, RAID 930-16i 8GB Flash PCIe 12Gb Adapter, 2x750W, XCC Enterprise, ThinkSystem Toolless Slide Rail, 7X99VGHQ00



Поз. №	Наименование Товара	Кол- во, всего (шт.)	Цена Товара за ед. без НДС (руб.)	Сумма Товара без НДС (руб.)	НДС		Сумма Товара с НДС (руб.)	Наименование производителя	Наименование Страны производителя	Наименование товара от производителя <sup>2</sup>
					Ставка %	Сумма НДС (руб.)				
	Platinum Hot-Swap Power Supply (AXE6) 2шт, 2.8m, 13A/100-250V, C13 to C14 Jumper Cord (6400) 2шт, ThinkSystem XClarity Controller Stand									
7	Сервер ThinkSystem SR650, форм фактор Rack 2U, в составе: SR650 3,5 Chassis with 8 or 12 bays (AUVW), Operating mode selection for: "Efficiency - Favoring Performance Mode" (BFYE), INTEL Xeon Gold 6230R 26C 150W 2.1GHz (BAZX) 2шт, ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM (B4H3) 8шт, ThinkSystem 2U 3.5" SATA/SAS 12-Bay Backplane (AUR9), select storage devices no configured RAID required (5977), ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E), ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD (B8HQ) 6шт, ThinkSystem M.2 with Mirroring Enablement Kit (AUMV), ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD (B8HS) 2шт, ThinkSystem 2U x8/x8/x8 PCIe FH Riser 1 (AUR4), ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter (AUZY), ThinkSystem Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter (AUKX), ThinkSystem 1100W (230V/115V) Platinum Hot-Swap Power Supply (AVWF) 2шт, 2.8m, 13A/100-250V, C13 to C14 Jumper Cord (6400) 2шт, ThinkSystem XClarity Contr	2	2 818 976,00	5 637 952,00	20	1 127 590,40	6 765 542,40	Lenovo	Китай	ThinkSystem SR650, 2xIntel Xeon Gold 6230R 26C 2.1GHz 150W, 8x32GB 2Rx4, 240GBx2 SATA, 6x3.84TB SSD, RAID 930-16i 8GB Flash PCIe 12G b Adapter, 2x1100W, XCC Enterprise, ThinkSystem Toolless Slide Rail, 7X06M3XY00
8	Сертификат на техническую поддержку (контракт сервисный) расширенную (Premium) программного обеспечения MaxPatrol SIEM (MP SIEM), в режиме 24x7, в течение 1 года, PT (POSITIVE TECHNOLOGIES) PT-MPSIEM-PRM-24x7-SUP	1	2 175 000,00	2 175 000,00	20	435 000,00	2 610 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Сертификат на расширенную техническую поддержку PREMIUM программного обеспечения MP SIEM, в режиме 24x7, в течение 1 (одного) года PT-MPSIEM-PR M-24x7-SUP



Поз. №	Наименование Товара	Кол-во, всего (шт.)	Цена Товара за ед. без НДС (руб.)	Сумма Товара без НДС (руб.)	НДС		Сумма Товара с НДС (руб.)	Наименование производителя	Наименование Страны производителя	Наименование товара от производителя <sup>2</sup>
					Ставка %	Сумма НДС (руб.)				
9	Сертификат на техническую поддержку (контракт сервисный) расширенную (Premium) программного обеспечения Network Attack Discovery (NAD), в режиме 24x7, в течение 1 года, PT (POSITIVE TECHNOLOGIES) PT-NAD-PRM-24x7-SUP	1	5 800 000,00	5 800 000,00	20	1 160 000,00	6 960 000,00	POSITIVE TECHNOLOGIES	Российская Федерация	Сертификат на расширенную техническую поддержку PREMIUM программного обеспечения NAD, в режиме 24x7, в течение 1 (одного) года PT-NAD-PRM-2 4x7-SUP
10	Пусконаладочные работы по внедрению, согласно заданию (Приложение №2)	1	5 865 377,00	5 865 377,00	20	1 173 075,40	7 038 452,40	ООО "БизКомм"	Российская Федерация	Создание системы оценки внутренних угроз и проведения аудита внутренних угроз
<b>ИТОГО:</b>				<b>61 934 211,00</b>	–	<b>6 006 842,20</b>	<b>67 941 053,20</b>	-	–	–

Условия поставки:

- В Стоимость Товара включены все расходы по поставке Товара.
- Стоимость тары, упаковки, реквизита, доставки (транспортных расходов, расходов на комплектацию, заготовительно-складских расходов) включена в стоимость.
- График работ и поставки:

№	Этап	Начало	Окончание	Общее время (в днях)
1	Поставка	03.03.2022	28.04.2022	40 (сорок) рабочих дней
2	Проектирование и внедрение	03.03.2022	30.06.2022	120 (сто двадцать) календарных дней

**Поставщик:**  
Заместитель генерального директора  
  
\_\_\_\_\_ Пестунов А.В.

**Покупатель:**  
Директор по информационным технологиям  
  
\_\_\_\_\_ Белокуров М.И.





### Задание на проектирование и внедрение

#### 1. Термины и сокращения

Сокращение	Описание
АРМ	Автоматизированное рабочее место
ВТСС	Вспомогательные технические средства и системы (систем)
ДО	Дочернее общество
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
КТС	Комплекс технических средств
ОТСС	Основные технические средства и системы (систем)
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
СКС	Структурированная кабельная система
Задание	Задание на проектирование и внедрение СЗПДн АО «Петербургская сбытовая компания»
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных

#### 2. Общие сведения

2.1. Наименование работ (номенклатура) и перечень объектов, на которых будут проводиться работы

Наименование работ: Проектирование и внедрение системы персональных данных (ИСПДн) АО "Петербургская сбытовая компания".

Место проведения работ АО "Петербургская сбытовая компания":

1. Центральный офис (ЦО) (195009, г. Санкт-Петербург, ул. Михайлова, д. 11);
2. Центр обработки данных (ЦОД) (197375 Санкт-Петербург, Репищева ул., д. 20а);

#### 2.2. Наименование системы

Полное наименование системы – Система защиты персональных данных АО «Петербургская сбытовая компания» (далее АО «Петербургская сбытовая компания»).

Условное обозначение (сокращенное обозначение) – СЗПДн.

#### 2.3. Требования к срокам проведения работ

Начало проведения работ – 03.03.2022;

Окончание проведения работ – 30.06.2022.

#### 2.4. Перечень организаций, участвующих в разработке СЗПДн

Заказчик – АО «Петербургская сбытовая компания» (далее – Заказчик).

Исполнитель – определяется на основании закупочной процедуры.

#### 2.5. Порядок предъявления Заказчику результатов работ

Порядок оформления и предъявления Заказчику результатов работ по рабочему проектированию СЗПДн и внедрению средств защиты информации (СрЗИ) определен в разделе 7 настоящего Задания на техно-рабочее проектирование СЗПДн и внедрение СЗИ (далее – Задание).

#### 3. Назначение и цели проведения работ

##### 3.1. Назначение работ

Назначением работ является разработка организационных и технических мероприятий по обеспечению информационной безопасности ПДн, а также информационных и/или автоматизированных систем и/или сетей связи, автоматизирующих процесс обработки ПДн.

##### 3.2. Цели проведения работ

Разработка техно-рабочего проекта СЗПДн АО «Петербургская сбытовая компания» в соответствии с единым подходом по защите информации в Группе компаний «Интер РАО», которое



позволит реализовать:

- Повышение уровня информационной безопасности ИСПДн путём реализации технических мероприятий по их защите.
- Исключение или существенное затруднение возможности несанкционированного получения, искажения, удаления злоумышленниками или случайными лицами защищаемой информации, обрабатываемой в ИСПДн, либо осуществления разрушающего воздействия на защищаемые данные и носители информации.
- Предотвращение несанкционированного доступа к защищаемой информации в ИСПДн и передачи её лицам, не имеющим права на доступ к такой информации.
- Своевременное обнаружение фактов/попыток несанкционированного доступа к защищаемой информации в ИСПДн.
- Недопущение воздействия на основные технические средства и системы обработки защищаемой информации, в результате которого нарушается их штатное функционирование.
- Обеспечение защиты информации от несанкционированного доступа при передаче её по каналам связи.

Внедрение СЗПДн АО «Петербургская сбытовая компания» в соответствии с единым подходом по защите информации в Группе компаний «Интер РАО», а также в соответствии с общим описанием СЗПДн, сформированным по результатам обследования ИТ инфраструктуры АО «Петербургская сбытовая компания» и разработанного техно-рабочего проекта с учетом типовых проектных решений, отраженных в п.3.2.1 настоящего Задания.

Выполнение требований законодательства Российской Федерации в части следующих законодательных актов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

#### 4. Характеристика объекта выполнения работ

##### 4.1. Границы проведения работ

Границей проведения работ по техно-рабочему проектированию СЗПДн являются ЦОД АО «Петербургская сбытовая компания».

В объем настоящего Задания на техно-рабочее проектирование входят следующие подсистемы СЗПДн:

- подсистема антивирусной защиты;
- подсистема межсетевого экранирования и обнаружения вторжений;
- подсистема защиты от атак 0 дня;
- подсистема защиты электронной почты;
- подсистема защиты среды виртуализации;
- подсистема защиты АРМ пользователей;
- подсистема защиты web-приложений;
- подсистема сбора и анализа событий безопасности;
- подсистема анализа защищенности.

В рамках работ в соответствии с настоящим Заданием необходимо:

- внедрить подсистему сбора и анализа событий безопасности, представленной в виде решения MaxPatrol SIEM



- внедрить РТ NAD
- внедрить подсистему защиты автоматизированных рабочих мест пользователей, реализованной с использованием встроенных механизмов ОС.

Полный перечень работ приведен в разделе «6. **Ошибка! Источник ссылки не найден.**».

#### 4.2. Текущее состояние информационных систем

На текущий момент в Группе компаний «Интер РАО» разработаны следующие документы, в рамках создания единого технического решения для Группы компаний «Интер РАО»:

- «Базовая модель угроз ИСПДн», ИРАО.ТТП.2020.006.МУ.001;
- «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001, который включает:
  - описание состава СЗПДн, перечня автоматизируемых функций и описание технических решений СЗПДн, архитектуры внедрения и требования по настройке СЗПДн, реализующих функцию безопасности;
  - обоснование выбора СрЗИ для каждой подсистемы СЗПДн;
  - требования к смежным системам;
  - логика применения мер защиты, в т.ч. конкретных моделей СрЗИ (содержит алгоритм, из которого следует необходимость в том или ином случае применять СрЗИ (в т.ч. конкретную модель), перечень обязательных и дополнительных мер защиты, а также критерии необходимости реализации дополнительных мер защиты;
- «Типовое техническое решение СЗПДн. Схема комплекса технических средств», ИРАО.ТТП.2020.008.КТС.001;
- «Типовое техническое решение СЗПДн. Ведомость оборудования и материалов», ИРАО.ТТП.2020.009.ВО.001.

В АО «Петербургская сбытовая компания» используются следующие типы ИСПДн:

- Централизованные ИСПДн – 7 шт.;
- ИСПДн АО «Петербургская сбытовая компания», как ИТ инфраструктура, с которой происходит подключение к внешним ИСПДн, а также другим Централизованным ИСПДн, имеющихся в компаниях группы «Интер РАО»;

Централизованные ИСПДн принадлежащие АО «Петербургская сбытовая компания» размещаются в:

- ЦОД АО «Петербургская сбытовая компания» по адресу г. Санкт-Петербург, ул. Репищева, дом 20 литера А (ДЦ Линкс), к ним относятся производственные системы, автоматизирующие энергосбытовую деятельность в части юридических и физических лиц.

### 5. Требования к выполнению работ

#### 5.1. Общие требования к работам

Объем проводимых работ включает:

- обследование текущего состояния ИБ и ИТ инфраструктуры Общества;
- ознакомление с частными моделями угроз ИСПДн АО «Петербургская сбытовая компания»;
- разработка документа «Общее описание настроек СЗИ»;
- разработка плана производства пуско-наладочных работ СрЗИ СЗПДн
- проведение пуско-наладочных работ подсистем СЗПДн, входящих в организационный объем настоящего Задания (в соответствии с пунктом 3.1.4 настоящего Задания)
- разработка Акта установки средств защиты информации;
- разработка документа «Программа и методика испытаний» для СЗПДн;
- проведение предварительных испытаний СЗПДн в соответствии с разработанным, согласованным и утвержденным Заказчиком документом «Программа и методика испытаний»;
- подготовка проекта Акта о приемке в опытную эксплуатацию СЗПДн;
- сопровождение СЗПДн на период опытной эксплуатации;
- подготовка проекта Акта о завершении опытной эксплуатации СЗПДн;
- проведение приемочных испытаний СЗПДн в соответствии с документом «Программа и методика испытаний»;
- подготовка проекта Акта о приемке в промышленную эксплуатацию СЗПДн;
- актуализация проектной документации в составе:



- Общее описание настроек СЗИ;
- Схема комплекса технических средств;
- Ведомость оборудования и материалов;
- Планы расположения оборудования;
- Чертежи установки технических средств;
- Схема сети уровня L2 и L3;
- Таблица соединений и подключений;

Детальное описание требований к составу и содержанию работ представлены в разделе 5 настоящего документа.

Работы должны выполняться с соблюдением нормативно-правовых актов РФ в области защиты информации и обработки ПДн:<sup>3</sup>

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Методические рекомендации «по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждены руководством 8 Центра ФСБ России № 149/7/2/6-432 от 31 марта 2015 года.

При проведении работ по настоящему Заданию исполнитель должен руководствоваться существующими документами в рамках типового технического решения СЗПДн для Группы компаний «Интер РАО», приведенными в пункте 4.2. настоящего Задания.

Технические решения СЗПДн АО «Петербургская сбытовая компания» не должны противоречить техническим решениям описанных в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.

## 5.2. Требования к составу работ

Работы по проектированию СЗПДн включают в себя:

- Обследование текущего состояния ИСПДн и ИТ инфраструктуры Общества:
  - сбор исходных данных об ИСПДн;
  - сбор сведения об имеющихся СРЗИ;
  - сбор исходных данных ИТ-инфраструктуре и инженерной инфраструктуры.
- Анализ частных моделей угроз и ВНД АО «Петербургская сбытовая компания»;
- Техно-рабочее проектирование СЗПДн:
  - разработка техно-рабочего проекта СЗПДн;
  - разработка эксплуатационной документации на СЗПДн.

Для проведения работ по подготовке ко вводу СЗПДн в действие специалисты Исполнителя допускаются на объект автоматизации Заказчика для проведения работ по установке и настройке программно-аппаратных и программных средств, а также согласования предлагаемых технических решений.

Остановка компонентов систем объекта автоматизации при выполнении работ по внедрению

<sup>3</sup> В случае опубликования и/или вступления в силу новых нормативно правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных, и/или внесения изменений в действующие нормативно-правовые акты, регламентирующие вопросы обеспечения безопасности персональных данных, в ходе выполнения работ они также должны быть учтены при выполнении работ.





осуществляется по согласованию с Заказчиком.

Для внедрения СЗПДн в части информационно-технологической инфраструктуры организации Заказчиком должны быть выполнены следующие мероприятия:

- осуществление мероприятий по модернизации инфраструктуры в рамках реализации требований к смежным системам, определенных в документе «Типовое ДО. Пояснительная записка» (в случае несоответствия инфраструктуры Общества указанным требованиям);
- закупка оборудования и ПО, обеспечивающего реализацию технического решения, описанного в документе «Типовое ДО. Пояснительная записка», согласно документу «Типовое ДО. Ведомость оборудования и материалов» в части подсистем, входящих в организационный объем работ по Заданию;
- создание комиссий для проведения предварительных и приемочных испытаний, приемки системы в опытную и промышленную эксплуатацию.

Детальное описание требований к составу работы отражены в разделе 6 настоящего Задания.

### 5.3. Место проведение работы

Работы по обследованию оборудования систем и сервисов, входящих в организационный объем, должны проводиться путем заполнения работниками АО «Петербургская сбытовая компания» опросного листа, подготовленного Исполнителем и последующего анализа полученных данных Исполнителем.

В случае необходимости Исполнителю уточнить сведения, указанные в опросном листе, Заказчик обеспечивает возможность проведения аудио/видео-конференц-связи с работниками АО «Петербургская сбытовая компания». По результатам аудио/видео-конференцсвязи Исполнитель должен внести уточненную информацию в опросный лист.

Пуско-наладочные работы СЗПДн оборудования систем и сервисов, входящих в организационный объем, проводятся в ЦОД АО «Петербургская сбытовая компания» по адресу г. Санкт-Петербург, ул. Репищева 20 литера А ДЦ Линкс, а также на площадке административного аппарата, расположенного по адресу г. Санкт-Петербург, ул. Михайлова, д.11.

### 5.4. Требования к структуре и функциям подсистем СЗПДн

В состав создаваемой СЗПДн должны входить следующие подсистемы:

- подсистема антивирусной защиты;
- подсистема межсетевого экранирования и обнаружения вторжений (ПМЭиОВ);
- подсистема защиты от атак 0 дня;
- подсистема защиты электронной почты;
- подсистема защиты среды виртуализации;
- подсистема защиты автоматизированных рабочих мест пользователей;
- подсистема защиты web-приложений;
- подсистема сбора и анализа событий безопасности;
- подсистема анализа защищенности.

Техническое решение в рамках Техно-рабочего проекта АО «Петербургская сбытовая компания» не должно противоречить техническому решению, описанному в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.

Во избежание дублирования средств защиты информации при проектировании СЗПДн должно быть учтено наличие в АО «Петербургская сбытовая компания» следующих функционирующих подсистем защиты информации, не противоречащих техническим решениям, описанным в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001:

- подсистема антивирусной защиты;
- подсистема межсетевого экранирования и обнаружения вторжений;
- подсистема защиты электронной почты;
- подсистема защиты среды виртуализации;
- подсистема защиты АРМ пользователей;
- подсистема анализа защищенности.

На стадии общего описания настроек СЗИ проекта должна быть проведена оценка достаточности существующих подсистем в части требуемой производительности, количества лицензий и соответствия техническим решениям, описанным в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.

При разработке общего описания настроек СЗИ должна быть учтена частная модель угроз в части скорректированных мер защиты. В случае если количество мер



набора в базовой модели угроз, количество средств защиты может быть скорректировано в меньшую сторону. При этом в рамках настоящего Задания на техно-рабочее проектирование количество средств защиты не может быть скорректировано в большую сторону относительно перечня средств защиты, описанного в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.

Подсистемы КСЗИ АО «Петербургская сбытовая компания» для Централизованных ИСПДн должны реализовывать функции, нейтрализующие или снижающие вероятность реализации угрозы безопасности информации, отраженных в приложении 2 «Перечень мер защиты для нейтрализации актуальных угроз УБИ для Централизованных ИСПДн и локальных ИСПДн, к которым предоставляется доступ иным юридическим лицам во исполнение договорных обязательств.

В состав подсистемы антивирусной защиты должны входить:

- компонент антивирусной защиты АРМ пользователей;
- компонент антивирусной защиты среды виртуализации.

В состав компонента антивирусной защиты АРМ пользователей подсистемы антивирусной защиты должны входить:

- модуль централизованного управления компонентом;
- модуль локального управления компонентом;
- модуль антивирусной защиты АРМ;
- модуль администрирования.

В состав компонента антивирусной защиты среды виртуализации подсистемы антивирусной защиты должны входить:

- модуль управления компонентом;
- модуль антивирусной защиты гипервизора.

В состав подсистемы межсетевого экранирования и обнаружения вторжений должны входить:

- компонент защиты периметра;
- компонент централизованного управления;
- компонент централизованного сбора событий.

В состав подсистемы защиты от атак 0 дня должны входить:

- компонент анализа в АО «Петербургская сбытовая компания».

В состав подсистемы защиты электронной почты должны входить:

- компонент защиты входящего почтового трафика;
- компонент защиты исходящего почтового трафика.

Подсистема защиты среды виртуализации должна быть реализована за счет использования встроенных механизмов среды виртуализации, прошедших процедуру оценки соответствия в форме приемочных испытаний.

Подсистема защиты АРМ пользователей должна быть реализована за счет использования встроенных механизмов ОС, прошедших процедуру оценки соответствия в форме приемочных испытаний или имеемого в наличии ПО SecretNetStudio.

В состав подсистемы защиты web-приложений должны входить:

- компонент защиты web-приложений, опубликованных в сети Интернет;
- компонент защиты внутренних web-приложений.

В состав подсистемы сбора и анализа событий безопасности должны входить:

- компонент централизованного управления подсистемой;
- компонент анализа событий безопасности;
- компонент сбора событий безопасности;
- компонент хранения событий.

В состав подсистемы анализа защищенности должны входить:

- компонент консолидации;
- компонент управления;
- сканер безопасности.

## 5.5. Требования к функциям, выполняемым СЗПДн

### 5.5.1. Подсистема антивирусной защиты

#### 5.5.1.1. Компонент антивирусной защиты АРМ пользователей

Компонент антивирусной защиты АРМ пользователей должен обеспечивать реализацию следующих функций:



- обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов;

- автоматическое обновление антивирусных баз и программных модулей по расписанию;
- формирование и рассылка отчетов о результатах проверки, по результатам обновлений и результатам работы постоянной защиты как вручную, так и по заданному расписанию;
- протоколирование результатов работы и действий эксплуатирующего персонала;
- передача информации о событиях на АРМ пользователей в подсистему сбора и анализа событий безопасности;

- централизованный сбор и хранение событий информационной безопасности, поступающих от клиентского ПО компонента антивирусной защиты АРМ пользователей;

- централизованное управление политиками и задачами антивирусной защиты;
- централизованный мониторинг состояния антивирусной защиты;
- интеграция сервера управления решением с Active Directory получения информации о рабочих станциях и серверах;

- реализация ролевая модель доступа к интерфейсам управления;
- встроенная система обнаружения сетевых атак;
- реализация защиты от эксплойтов;
- реализация защиты от программ-вымогателей;
- предотвращение бесфайловых атак;
- обнаружение угроз на основе машинного обучения;
- реализация возможности отката последствий заражения вредоносного ПО.

Реализация компонента должна учитывать наличие существующих серверов управления с ПО Kaspersky Security Center. На этапе техно-рабочего проектирования необходимо предусмотреть возможность использования данных серверов.

Модуль локального управления компонента антивирусной защиты АРМ пользователей должен обеспечивать централизованное управление модулем антивирусной защиты АРМ

Модуль локального управления компонента должен быть подчинен модулю централизованного управления компонентом, находящегося в ЦОД БЦ ЛУЧ.

Должна быть обеспечена интеграция модуля локального управления компонентом с доменом Active Directory intterrao.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления модуля.

#### 5.5.1.2. Компонент антивирусной защиты среды виртуализации

Компонент антивирусной защиты среды виртуализации должен обеспечивать реализацию следующих функций:

- обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на виртуальной машине объектов на присутствие вирусов) и проверки по требованию;

- автоматическое обновление антивирусных баз и программных модулей по расписанию;
- возможность применять различные параметры безопасности для отдельных групп виртуальных машин;

- формирование и рассылка отчетов о результатах проверки, по результатам обновлений и результатам работы постоянной защиты как вручную, так и по заданному расписанию;

- протоколирование результатов работы и действий эксплуатирующего персонала;
- передача информации о событиях на виртуальных машинах в подсистему сбора и анализа событий безопасности;

- централизованный сбор и хранение событий информационной безопасности, поступающих от модуля антивирусной защиты гипервизора;

- реализация безагентской антивирусной защиты виртуальных машин;
- использование выделенных виртуальных машин для задач сканирования данных на наличие вредоносного кода;

- реализация оптимизации проверки с помощью технологии общего кэша Shared Cache;
- обеспечение проверки на наличие вредоносного кода всех объектов запускаемых, открываемых и сохраняемых;



- возможность интеграции с VMware vCenter/выделенном VMware ESXi сервером.

Реализация компонента должна учитывать наличие существующих серверов управления с ПО Kaspersky Security Center. На этапе техно-рабочего проектирования необходимо предусмотреть возможность использования данных серверов.

Должна быть обеспечена интеграция модуля управления компонентом с доменом Active Directory interra.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления модуля.

#### 5.5.2. Подсистема межсетевого экранирования и обнаружения вторжений

##### 5.5.2.1. Компонент защиты периметра АО «Петербургская сбытовая компания»

Компонент защиты периметра в АО «Петербургская сбытовая компания» подсистемы межсетевого экранирования и обнаружения вторжений должен обеспечивать реализацию следующих функций:

- фильтрация сетевых пакетов с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов (антиспуфинг);
- фильтрация сетевого трафика при взаимодействии АРМ пользователей с сегментами размещения серверов АО «Петербургская сбытовая компания»;
- фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктур;
- фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления подсистем СЗПДн;
- контроль доступа в сеть Интернет;
- регистрация фактов установления сетевых сессий;
- идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH;
- регистрация событий фильтрации трафика и передача в компонент централизованного сбора событий действий администратора за сеанс;
- инспекция информационных потоков, организуемых с серверами защищаемых ИСПДН на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты;
- анализ сетевой активности защищаемых сегментов Общества с использованием баз сигнатур, предоставленных производителем оборудования;
- автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»);
- регистрация событий обнаружения опасной сетевой активности;
- фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- контроль приложений (шейпинг, приоритизация, дроп), мониторинг и управление доступом к внешним ресурсам;
- противодействие DDOS-атакам;
- потоковая антивирусная защита;
- мониторинг веб-трафика, ограничение доступа к конкретным источникам (URL-фильтрация), фильтры приложений;
- инспекция HTTPS-трафика.

Для компонента защиты периметра в АО «Петербургская сбытовая компания» должна быть разработана сетевая матрица доступа в соответствии со следующими критериями:

- обеспечение разграничения сетевого доступа сотрудников Заказчика по учетным записям домена Active Directory к защищаемым ИС с учетом их функциональных обязанностей;
- обеспечение контроля сетевого взаимодействия ИС со смежными системами для обеспечения функционирования программно-технических средств ИС;
- обеспечение функционирования программно-технических средств подсистем защиты, входящих в состав СЗПДн.

Формирование сетевой матрицы доступа должно выполняться с учетом обеспечения минимально-необходимого взаимодействия для обеспечения функционирования ИС.

Исполнителем должна быть разработана сетевая матрица доступа на основании данных,





предоставленных Заказчиком. Перечень данных должен быть сформирован Исполнителем на этапе проведения обследования

Должны быть настроены параметры SNMP-протокола компонента защиты периметра в АО «Петербургская сбытовая компания» подсистемы межсетевого экранирования и обнаружения вторжений для возможности его мониторинга существующими системами Заказчика.

#### 5.5.2.2. Компонент централизованного управления

Компонент централизованного управления подсистемы межсетевого экранирования и обнаружения вторжений должен обеспечивать реализацию следующих функций:

- настройка политик межсетевого экранирования, обнаружения и предотвращения вторжения на управляемых компонентах защиты периметра;
- мониторинг работы всех компонентов подсистемы;
- настройка политик безопасности для доступа между сетевыми сегментами Общества;
- управление компонентом защиты периметра с использованием протоколов, защищенных от возможности прослушивания паролей и другой существенной информации;
- возможность группировки управляемых устройств для назначения политик по отдельным группам;
- возможность назначения глобальных политик безопасности, которые могут применяться ко всем управляемым устройствам одновременно;
- поддерживать администрирование на основе ролей;
- поддерживать несколько уровней администраторов и пользователей;
- поддерживать управление через Web-интерфейс;
- централизованное управление распределенными устройствами;
- интеграция с Active Directory для настройки групп безопасности и разграничения доступа.

Должна быть обеспечена интеграция модуля централизованного управления с доменом Active Directory interra.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления.

#### 5.5.2.3. Компонент централизованного сбора событий

Компонент централизованного сбора событий подсистемы межсетевого экранирования и обнаружения вторжений должен обеспечивать реализацию следующих функций:

- ведение журналов событий информационной безопасности и осуществлять их индексирования для быстрого поиска;
- прием и обработка событий ИБ, получаемых с компонента защиты периметра в АО «Петербургская сбытовая компания»;
- прием и обработка событий ИБ, полученный от подсистемы защиты электронной почты;
- прием и обработка событий ИБ, полученных от подсистемы защиты web-приложений;
- прием и обработка событий ИБ, полученных от подсистемы защиты от атак 0 дня;
- возможность просмотра событий ИБ в реальном времени;
- возможность поиска и фильтрации данных в событиях ИБ;
- автоматическая подготовка настраиваемых графических отчетов по сетевой активности, системным событиям, вирусам, атакам, web-фильтрации;
- возможность подготовки формирования подготовленных отчетов по расписанию;
- обеспечение хранения полученных событий информационной безопасности для последующей ретроспективной отчетности;
- возможность создания оповещений при возникновении определённых событий.
- передача событий безопасности в подсистему сбора и анализа событий безопасности;
- централизованное управление статистикой (журналами событий), формирование отчетности и оповещения.

Должна быть обеспечена интеграция компонента централизованного сбора событий с доменом Active Directory interra.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления.

#### 5.5.3. Подсистема защиты от атак 0 дня

Подсистема защиты от атак 0 дня должна обеспечивать реализацию следующих функций:



- выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак;
- возможность предоставления отчетов по результатам анализа, включающих выявленные признаки угрозы;
- возможность интеграции с подсистемой защиты электронной почты в части получения контента для анализа;
- возможность ручной загрузки файлов на компоненты анализа файлов;
- возможность использования преднастроенных образов виртуальных машин;
- централизованная система управления;
- возможность блокировки почтового трафика;
- анализ HTTP/HTTPS;
- эмуляция подозрительных файлов;
- эмуляция скриптов;
- эмуляция макросов;
- проверка архивов с паролем (словарные пароли);
- проверка веб-ссылок в теле письма и в документе;
- поддержка ОС семейства Microsoft Windows в образах виртуальных машин (песочниц);
- система сокрытия работы в виртуальной среде (Anti-VM evasion protection);
- ретроспективный анализ событий;
- поддержка динамического анализа одновременно в нескольких ОС локально на устройстве (Multi-Version);
- поддержка динамического анализа одновременно с несколькими версиями прикладного ПО локально на устройстве (Multi-Version);
- выявление многовекторных атак — Multi-Vector Attack;
- обнаружение сложных составных атак с доставкой вредоносного кода по частям с разных внешних ресурсов — Multi-Flow Attack;
- машинное обучение для обнаружения угроз и аномалий;
- возможность предоставления отчетов по результатам анализа, включающих выявленные признаки угрозы.

#### 5.5.4. Подсистема защиты электронной почты

Подсистема защиты электронной почты должна обеспечивать реализацию следующих функций:

- анализ почтового трафика на предмет наличия вредоносных вложений и нежелательных электронных писем, ссылок на опасные сайты;
- отправка на проверку вложенных в электронные письма файлы в подсистему защиты от атак 0 дня;
- реализация механизмов проверки репутации отправителя, протокола, содержимого письма, репутации IP-адреса домена;
- возможность работы в качестве шлюза электронной почты (MTA – mail transfer agent);
- возможность предоставления отчетов и статистики по результатам работы подсистемы;
- централизованное управление;
- возможность интеграции с LDAP для формирования политик и проверки получателей;
- реализация защиты от Directory Harvest Attack;
- реализация защиты от Bounce-атак;
- анализ изображений на наличие спама;
- возможность помещение зараженных объектов на карантин;
- возможность управления сообщениями в карантине через SMTP.

Должна быть обеспечена интеграция подсистемы защиты электронной почты с доменом Active Directory interra.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления.

#### 5.5.5. Подсистема защиты среды виртуализации

Для обеспечения защиты среды виртуализации от несанкционированного доступа, а также для закрытия актуальных угроз с помощью встроенных в решения по построению среды виртуализации механизмов должны быть описаны и детализированы следующие компенсирующие меры:



- для всех учетных записей администраторов виртуальной инфраструктуры и администраторов ИБ используются пароли, длина и сложность которых соответствует действующей в Группе компаний «Интер РАО» парольной политике;

- авторизация администраторов виртуальной инфраструктуры и администраторов ИБ осуществляется через единый каталог Active Directory и с использованием локальных учетных записей;

- выделение трех типов учетных записей администраторов виртуальной инфраструктуры:

- учетные записи администраторов с расширенными правами – локальные учетные записи системы виртуализации, которые имеют расширенные права доступа (например, изменение конфигурации серверов виртуализации, удаление виртуальных машин/дисков, доступ к дисковым хранилищам серверов виртуализации);

- учетные записи администраторов с ограниченными правами – учетные записи из каталога Active Directory, которые имеют ограниченные права доступа, необходимые для выполнения регулярных административных операций, таких как: создание виртуальных машин, изменение параметрами виртуальных машин, запуск/остановка виртуальных машин;

- сервисные учетные записи виртуальной инфраструктуры – локальные учетные записи системы виртуализации, которые имеют минимально необходимый доступ только к необходимым для данной учетной записи объектам виртуальной инфраструктуры;

- все учетные записи администраторов виртуальной инфраструктуры ограничены минимально необходимым доступом к функциям и объектам виртуальной инфраструктуры в соответствии со служебными обязанностями конкретного администратора;

- средствами ПМЭиОВ настраивается минимально необходимый доступ к компонентам виртуальной инфраструктуры;

- настраивается дискретный доступ к компонентам виртуальной инфраструктуры с минимально необходимыми правами доступа для пользователя виртуальной инфраструктуры;

- осуществляется централизация управления виртуальной инфраструктурой через vCenter для виртуальной инфраструктуры на базе VMware и SCVMM для виртуальной инфраструктуры на базе Hyper-V;

- для обеспечения оперативного реагирования на инциденты ИБ на технических средствах подсистемы сбора и анализа событий информационной безопасности осуществляется сбор событий ИБ с компонентов виртуальной инфраструктуры;

- реализуется запрет непосредственного доступа к управлению компонентами виртуальной инфраструктуры по протоколам удаленного доступа (SSH, RDP);

- реализуется запрет прямого доступа программы управления виртуальной инфраструктурой к серверу виртуализации, минуя централизованный сервер управления виртуальной инфраструктурой;

- используются механизмы, обеспечивающие защиту образов виртуальных машин от несанкционированной модификации;

- синхронизация времени на всех компонентах виртуальной инфраструктуры с существующими доверенными NTP-серверами.

Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в подсистеме должна быть предусмотрена процедура аутентификации администраторов при доступе к интерфейсам управления средой виртуализации.

Должна быть обеспечена интеграция подсистемы с доменом Active Directory interrao.ru для аутентификации администраторов подсистемы при доступе к интерфейсу управления модулем и администраторов виртуальной инфраструктуры при доступе к интерфейсам управления виртуальной инфраструктуры.

#### 5.5.6. Подсистема защиты APM пользователей

Для обеспечения защиты от несанкционированного доступа виртуальных машин, работающих под управлением операционной системы семейства Linux, а также для закрытия актуальных угроз (угроза эксплуатации цифровой подписи программного кода и угроза несанкционированного восстановления удаленной защищаемой информации) должны быть описаны и детализированы следующие компенсирующие меры;

- с использованием штатных средств операционных систем семейства Linux осуществляется контроль целостности файлов (утилита «aide»);

- с использованием штатных средств операционных систем семейства Linux осуществляется затирание файлов (утилита «shred») и затирание блоков жесткого диска (утилита «dd»);



после удаления файлов с использованием перечисленных утилит у злоумышленника должна отсутствовать возможность восстановления этих файлов»

- для ограничения удаленного доступа к консоли управления виртуальными серверами по протоколу SSH на межсетевых экранах ПМЭиОВ настраиваются правила межсетевого экранирования, разрешающие доступ только по протоколу SSH (TCP/22) и только для IP-адресов АРМ системных администраторов и их доменных учетных записей;

- с использованием средств подсистемы сбора и анализа событий информационной безопасности осуществляется сбор журналов с серверов Linux. При попытке получения несанкционированного доступа к серверам Linux (ввод неверного пароля), а также ввода команд, подсистема сбора и анализа событий информационной безопасности получит соответствующую информацию, сгенерирует инцидент информационной безопасности (broot force) и отправит email-оповещение на электронный адрес администратора ИБ;

- аудит действий администраторов серверов настраивается с использованием штатных средств операционных систем семейства Linux (утилита «auditd»).

Для обеспечения защиты АРМ пользователей от несанкционированного доступа, а также для закрытия актуальных угроз с помощью встроенных в ОС механизмов и механизмов групповых политик Active Directory должны быть описаны и детализированы следующие компенсирующие меры:

- применение трехэтапного обновления операционной системы Windows на АРМ пользователей при помощи Microsoft System Center Configuration Manager:

- тестирование новых обновлений на АРМ пользователей тестовой группы (в течение 7 дней);
- распространение успешно протестированных обновлений на АРМ пользователей (в течение 7 дней);

- принудительная перезагрузка в нерабочее время АРМ пользователей, которые не установили распространяемое обновление;

- автоматическая блокировка экрана АРМ пользователя по причине неактивности пользователя и при извлечении токена;

- применение для доменных администраторов и пользователей домена различных парольных политик;

- установка единой парольной политики для всех доменных администраторов Группы компании «Интер РАО»:

- минимальная длина пароля – 16 символов;
- максимальный срок действия пароля – 30 дней;
- минимальный срок действия пароля – 5 дней;
- проверка сложности пароля должна быть включена;
- должно обеспечивать уникальность 15 последних паролей;
- блокировка учетной записи после 5 неудачных попыток авторизации;
- разрешить следующую попытку аутентификации через 180 минут;

- установка единой парольной политики для всех пользователей домена Группы компаний «Интер РАО»:

- минимальная длина пароля – 8 символов;
- максимальный срок действия пароля – 90 дней;
- минимальный срок действия пароля – 10 дней;
- проверка сложности пароля должна быть включена;
- должно обеспечивать уникальность 2 последних паролей;
- блокировка учетной записи после 10 неудачных попыток авторизации;
- разрешить следующую попытку аутентификации через 120 минут;

- ведение журналов событий входа (выхода) пользователей, доступа к ресурсам, запуск/остановка процессов;

- назначены минимально необходимые права доступа пользователей к управлению АРМ и файловой системе;

- должно быть отключено хранение хэш-значений LAN Manager при смене пароля;

- должно быть установлено требование 128-битного шифрования для сеансов безопасности на базе NTLM SSP (включая безопасный RPC);

- должна быть отключена отправка незашифрованных паролей сторонним SMB-серверам;

- должно быть включено обнаружение установки приложения и запросов на повышение прав;

- должно быть включено переключение к безопасному рабочему столу при выполнении запроса на повышения прав;



- при запросе повышения прав для обычных пользователей должен быть активирован запрос учетных данных на безопасном рабочем столе;
- должен быть включен запрет перечисления учетных записей SAM анонимными пользователями;
- должен быть включен запрет пользователям на установку драйвера принтера;
- должны быть отключены встроенные учетные записи «Администратор» и «Гость»;
- должно быть включено требование цифровой подписи или шифрования потока данных безопасного канала при взаимодействии с контроллером домена.

#### 5.5.7. Подсистема защиты web-приложений

Подсистема защиты web-приложений должна обеспечивать реализацию следующих функций:

- поддержка механизмов предотвращения использования известных уязвимостей в ПО (virtual patching);
- противодействие типовым угрозам для web-приложений:
  - HTTP-атаки, включая атаки на переполнение буфера;
  - противодействие брутфорс-атакам (подбор паролей);
  - защита от мошенничества (проверка привязки к сессии пользователя, детектирование автоматизированной активности);
  - защита от роботов, включающая наличие встроенной базы роботов и автоматическое поведенческое детектирование робота
- защита cookie (в том числе флаг HttpOnly);
- защита от HPP (HTTP Parameter Pollution — смешивание («загрязнение») границ HTTP-параметров);
- защита от HTTP Verb Tampering;
- защита от OS Commanding;
- защита от сложных клиентских атак Clickjacking;
- обнаружение сложных атак на стороне клиента XSS, CSRF/XSRF;
- защита от атак типа DOM-based XSS;
- обеспечение противодействия угрозам из списка OWASP TOP 10;
- инъекции (A1 — Injection);
- нарушение авторизации и управления сессией (A2 — Broken Authentication and Session Management);
- межсайтовое выполнение сценариев (A3 — Cross-Site Scripting (XSS));
- небезопасные прямые ссылки на объект (A4 — Insecure Direct Object References);
- ошибки настройки параметров безопасности (A5 — Security Misconfiguration);
- раскрытие чувствительных данных (A6 — Sensitive Data Exposure);
- отсутствие контроля уровня доступа к функции (A7 — Missing Function Level Access Control);
- подделка межсайтовых запросов (A8 — Cross-Site Request Forgery (CSRF));
- использование компонентов с известными уязвимостями (A9 — Using Components with Known Vulnerabilities);
- непроверенные перенаправления (A10 — Unvalidated Redirects and Forwards);
- нормализация HTTP-запросов с учетом особенностей используемого веб-сервера для защищаемого приложения;
- выявление отклонений от типовой модели для данного приложения (от профиля);
- анализ поведения пользователя приложения и автоматическое обнаружение пользователей с аномальным поведением;
- определение автоматизированных действий пользователя;
- определение доверенности адреса (на основе черных списков);
- возможность автоматизированного эвристического механизма самообучения, включающего анализ входных данных от пользователя, учитывающего тип каждого символа и порядок типов символов и спецсимволов;
- передача событий безопасности в подсистему сбора и анализа событий безопасности;
- терминирование SSL/TLS соединений при терминировании клиентом во всех режимах работы;
- реализация функций валидации:
  - с фильтрацией пакетов на основе битовой маски;
  - строгая проверка методом на соответствие RFC путем проверки дублирования заголовков;





- проверка на основе ограничений используемых версий протокола, количества заголовков, количества cookies;
- анализ протокола HTTP;
- анализ протокола HTTPS;
- анализ протокола SOAP;
- анализ протокола XML;
- анализ протокола JSON;
- поддержка ГОСТ шифрования при использовании функционала терминирования SSL;
- централизованное управление распределенными устройствами;
- системами управления учётными записями посредством протоколов LDAP или RADIUS;
- реализация ролевой модели доступа администраторов к системе;
- поддержка протоколы отправки данных/журналов событий:
- syslog;
- SNMP;
- приоритизация событий (приоритет, тип);
- агрегирование событий (группировка однотипных событий);
- создание отчётов на основе зарегистрированных событий.

#### 5.5.8. Подсистема сбора и анализа событий безопасности

Подсистема сбора и анализа событий безопасности должна выполнять следующие функциональные задачи:

- регистрация событий ИБ от подсистем СЗПДн и объектов ИТ-инфраструктуры Общества;
- сбор, обработку и хранение зарегистрированных событий ИБ.

В рамках реализации задачи по регистрации событий ИБ должны выполняться следующие функции (при наличии данной информации в raw-событиях с источников событий):

- регистрация входа/выхода субъектов доступа к защищаемым ресурсам, с указанием следующих параметров:
  - дата и время входа/выхода субъекта доступа в систему/из системы или загрузки/остановки системы,
  - результат попытки входа (успешная/неуспешная),
  - идентификатор субъекта, предъявленный при попытке доступа;
- регистрация запуска и завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов, с указанием следующих параметров:
  - дата и время запуска/завершения программы или процесса (задания, задачи), предназначенных для обработки защищаемых файлов,
  - идентификатор субъекта, осуществившего запуск/завершение программы или процесса (задания, задачи), предназначенных для обработки защищаемых файлов;
- регистрация попыток доступа субъектов (пользователей и процессов) к защищаемым объектам доступа (файлам, каталогам), с указанием следующих параметров:
  - дата и время попытки доступа субъекта к объектам доступа,
  - результат попытки доступа (успешная/неуспешная),
  - идентификатор субъекта, осуществившего попытку доступа к объекту;
- сбор, запись и хранение зарегистрированных событий безопасности в течение установленного времени хранения.

В рамках реализации задач по сбору, обработке и хранению событий ИБ должны выполняться следующие функции:

- сбор событий ИБ должен осуществляться по следующим протоколам/способам (конкретный протокол определяется на этапе разработки рабочей документации с учетом функциональных возможностей источника событий):
  - Syslog;
  - MS Windows Event log (wmi);
  - СУБД с использованием ODBC.
- обработку получаемых событий ИБ, включая:
  - фильтрации;
  - нормализации;



- агрегации;
- категоризации;
- приоритезации;
- корреляции.
- хранение событий должно выполняться в линейно масштабируемой нереляционной СУБД (noSQL);
- визуализацию топологии сети, включая построение на актуальный момент времени топологии сети;
- ведение базы активов:
- перечня объектов с присущими данному объекту определенных характеристик (АРМ, сервера, узлы сети, пользователи, группы пользователей и т.п.);
- обнаружение и добавление активов следующими способами: анализом событий, активным сканированием (тестирование на проникновение, системные проверки), анализом сетевого трафика, импорт из Active Directory, добавление актива «вручную»;
- сканирование узлов сети, включая:
- инвентаризационное сканирование в целях выявления, идентификации узлов сети, а также получения их характеристик;
- сетевое сканирование в целях идентификации сетевых служб.
- автоматическую актуализацию информации об активах по результатам сканирования узлов сети;
- корреляцию событий ИБ, включая:
- корреляцию событий ИБ на основе встроенной базы правил корреляции;
- возможность создания собственных правил корреляции;
- возможность использования в правилах корреляции перечня заведенных в подсистеме активов;
- возможность использования справочников при формировании правил корреляции;
- многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.
- возможность оптимизации правил корреляции с использованием новых данных об активах;
- возможность управления задачами по сбору, обработке и корреляции событий, управления активами из единой консоли (web-интерфейса);
- неограниченного увеличения объемов хранения (в части отсутствия лицензионного ограничения);
- возможность интеграции с решениями других производителей через открытый API;
- отсутствие лицензионных ограничений на кол-во и объем поступающих событий;
- возможность подключения новых источников событий ИБ, в том числе систем ИС.

К подсистеме должны быть подключены источники событий, входящие в состав СЗПДн.

Подключение источников событий должно выполняться с учетом функциональных возможностей используемого ПО в подсистеме.

Реализация подсистемы должна учитывать существующие решения Заказчика, которые не противоречат техническим решениям, описанным в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.

#### 5.5.9. Подсистема анализа защищенности

Подсистема анализа защищенности должна обеспечивать реализацию следующих функций:

- инвентаризация объектов ИТ-инфраструктуры Общества;
- выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам
- выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам;
- выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов;
- выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений;
- выявление учетных записей с паролями, содержащимися в справочниках, задаваемых администратором в настройках сканирования (словарными паролями);
- сбор сведений о составе программного и аппаратного обеспечения сканируемого узла;



- сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла;
- сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации;
- формирование отчетов по результатам сканирований;
- централизованное управление элементами подсистемы и доступом пользователей к элементам подсистемы.

#### 5.6. Требования к численности и квалификации персонала СЗПДн и режиму его работы

Уровень квалификации персонала СЗПДн должен обеспечивать выполнение возложенных на них функциональных обязанностей, которые должны быть отражены в пояснительной записке к техно-рабочему проекту СЗПДн Общества.

Уровень квалификации персонала СЗПДн должен быть достаточным для реализации всех функций (автоматизированных и автоматических) системы во всех режимах ее работы.

Требования к численности, функциональным обязанностям ролей эксплуатационного персонала и ролей пользователей должны быть актуализованы в Пояснительной записке к техно-рабочему проекту СЗПДн Общества в соответствии с документом «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001 и с учетом актуального набора подсистем СЗПДн Общества.

Роли и функции обслуживающего персонала должны быть определены с учетом разграничения ответственности между работниками, осуществляющими централизованную эксплуатацию и экспертную (аналитическую) поддержку системы защиты и работниками, отвечающими за эксплуатацию подсистем защиты информации на месте (в ДО).

Для подсистем, находящихся в зоне ответственности подразделения, занимающегося обеспечением информационной безопасности и подразделений, занимающихся поддержкой ИТ-инфраструктуры, должны быть определены зоны разграничения ответственности.

#### 5.7. Требования к надежности

При разработке техно-рабочего проекта АО «Петербургская сбытовая компания» должны учитываться показатели надежности для каждой подсистемы реализуемые в рамках документа «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001. Для подсистем, не предполагающих наличия резервирования по схеме N+1, в рамках техно-рабочего проекта АО «Петербургская сбытовая компания» должно быть указано время восстановления работоспособности в случае сбоя.

Должно быть предусмотрено сохранение накопленной информации (журналы работы и конфигурационные файлы компонент СЗПДн) на случай сбоя в подсистемах СЗПДн с последующим восстановлением функционирования СЗПДн после проведения ремонтных и восстановительных работ. Проектные решения по сохранению информации должны учитывать используемые у заказчика системы резервного копирования. В случае отсутствия у заказчика системы резервного копирования, то в рамках проектного решения предоставляются требования к системе резервного копирования, которая должны быть внедрены заказчиком к моменту внедрения СЗПДн.

Отказоустойчивость подсистем СЗПДн должна обеспечиваться за счет использования программных и программно-аппаратных решений, поддерживающих резервирование компонентов.

Отказоустойчивость компонентов управления подсистемами СЗПДн должна обеспечиваться за счет использования отказоустойчивых конфигураций (кластеров), либо за счет использования средств среды виртуализации Заказчика.

В подсистемах СЗПДн должна быть обеспечена сохранность информации при авариях, отказе технических средств, потере питания.

Сохранность информации при авариях должна быть обеспечена за счет хранения резервных копий настроек программного обеспечения компонентов подсистем СЗПДн.

Резервное копирование и архивация конфигураций подсистем СЗПДн должны осуществляться штатными средствами Заказчика или средствами самих подсистем.

При авариях и сбоях в работе оборудования должна быть обеспечена возможность восстановления настроек компонентов подсистем СЗПДн из резервных копий.

#### 5.8. Требования по обеспечению информационной безопасности

Для всех подсистем СЗПДн должна быть предусмотрена возможность регистрации событий, в которых должна отражаться информация по входу/выходу администраторов подсистем, а также по событиям, совершенным с использованием административных полномочий.

Для всех подсистем СЗПДн механизмы протоколирования должны обеспечивать возможность



записи и хранения следующей информации<sup>4</sup> (включая но не ограничиваясь):

- дата (день, месяц, год) и время (часы, минуты, секунды) действия/события;
- идентификатор пользователя;
- IP-адрес пользователя /источника события;
- тип действия/события;
- результаты выполнения действия/события: успешное или неуспешное.

#### 5.9. Требования к защите от внешних воздействий

В организационный объем работ по данному Заданию решения по защите от утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок к программно-техническим СрЗИ не входят.

#### 5.10. Требования к защите информации от несанкционированного доступа

Компоненты управления подсистем СЗПДн должны обеспечивать:

- аутентификацию администраторов подсистем, на основе персонифицированной учетной записи пользователя и пароля;
- авторизацию администраторов подсистем, на основе назначенных учетной записи функциональных ролей;
- исключение анонимного доступа пользователей;
- разграничение прав доступа администраторов подсистем и пользователей подсистем в соответствии с их функциональными обязанностями;
- закрытие текущей сессии и повторное выполнение процедур аутентификации и авторизации в случаях нарушения или разрыва соединения.

Во всех подсистемах СЗПДн должны использоваться персонифицированные и уникальные идентификаторы (логины) для каждой учетной записи.

Во всех подсистемах СЗПДн при проведении аутентификации процедура проверки введенных пользователем данных должна выполняться только после того, как пользователь закончит ввод информации для аутентификации.

В целях обеспечения защиты информации, передаваемой по каналам связи для пользователей АО «Петербургская сбытовая компания», а также пользователей, имеющих доступ к ИСПДн из сети Интернет, должна быть обеспечена защита доступа к компонентам ИСПДн.

В СЗПДн, в случае такой необходимости и обоснованности, должны использоваться криптографические средства защиты, прошедшие процедуру оценки соответствия в форме обязательной сертификации на соответствие требованиям ФСБ России к средствам криптографической защиты информации.

#### 5.11. Требования к патентной чистоте

Технические решения по построению СЗПДн должны отвечать требованиям действующего законодательства Российской Федерации об авторском праве и смежных правах по патентной чистоте.

#### 5.12. Требования по стандартизации и унификации

Проектирование СЗПДн должно осуществляться в соответствии с единым подходом по защите информации в Группе компаний «Интер РАО».

Проектные решения по использованию технических средств и ПО системы должны предусматривать однотипные компоненты в целях обеспечения снижения расходов на обслуживание (эксплуатацию) и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

При проектировании необходимо учитывать принцип максимальной централизации администрирования технических средств и их совместимости с ИТ-инфраструктурой и с средствами защиты, размещенными в ЦОД «БЦ Луч».

Требования по стандартизации и унификации могут уточняться на этапе техно-рабочего проектирования СЗПДн.



## 6. Состав и содержание работ

Этапы, продолжительность и содержание работ приведены в таблице **Ошибка! Источник ссылки не найден.** «Этапы работ»

Таблица 1 – Этапы работ

№	Этап	Содержание работ	Отчетные документы (результат работ по этапу)	Сроки (не позднее)
1.	Обследование текущего состояния ИСПДн и ИТ инфраструктуры Общества			120 (сто двадцать) календарных дней
1.1.	Сбор исходных данных об ИСПДн	<p>Целью данного подэтапа является сбор сведений о каждой ИСПДн Заказчика и ИТ инфраструктуре в объеме достаточном реализовать типовое проектное решение по созданию СЗПДн.</p> <p>При сборе информации об ИСПДн Заказчика учитываются сведения, содержащиеся во внутренних документах Заказчика. Обследование ИСПДн выполняется путем заполнения Заказчиком опросного листа, разработанного Исполнителем, анализа проектной и эксплуатационной документации на ИСПДн и включают в себя:</p> <p>сбор информации об ИСПДн, в объеме сведения:</p> <ul style="list-style-type: none"> <li>категории обрабатываемых ПДн;</li> <li>объем обрабатываемых ПДн;</li> <li>категории субъектов ПДн и их состав;</li> <li>используемые технологии в ИСПДн.</li> </ul> <p>сбор сведений об информационных потоках в ИСПДн (в т.ч. информационных потоках с внешними системами и сетями связи), в объеме достаточном для разработки сетевой матрица доступа;</p> <p>сбор сведений о существующей ролевой модели разграничения доступа в ИСПДн;</p> <p>сбор сведений о способах доступа пользователей к ИСПДн;</p> <p>сбор информации о серверной инфраструктуре ИСПДн;</p> <p>сбор сведений по серверным помещениям и имеющемуся сетевому оборудованию (в объеме необходимом для разработки рабочей документации);</p> <p>на основании собранной информации необходимо определить уровень защищенности для каждой ИСПДн приведенной в приложении 1 к настоящему Заданию (результат определения УЗ необходимо отразить в отчете);</p> <p>для ИСПДн Типового ДО необходимо определить УЗ в соответствии с минимальным УЗ для ИСПДн используемых в Типовом ДО.</p>		
1.2.	Сбор сведения об имеющихся СрЗИ	На данном подэтапе проводится выявление применяемых в АО «Петербургская сбытовая компания» СрЗИ, которые соответствуют решениям, описанным в документе «Типовое техническое решение		





		СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001.		
1.3.	Сбор исходных данных ИТ-инфраструктуре и инженерной инфраструктуры	На данном подэтапе производится сбор сведений о количестве АРМ пользователей, сетевой, серверной и инженерной инфраструктуре Заказчика, в объеме необходимо для осуществления техно-рабочего проектирования.		
2.	Ознакомление с разработанными частными моделями угроз на ИСПДн АО «Петербургская сбытовая компания»			
3.	Техно-рабочее проектирование СЗПДн Типового ДО		Общее описание подходов по созданию СЗИ с учетом нюансов ИТ инфраструктуры в соответствии с типовыми проектными решениями, отраженными в документах из п.3.2.1. настоящего Задания	
3.1.	Разработка Общего описания подходов по созданию СЗИ с учетом нюансов ИТ инфраструктуры в соответствии с типовыми проектными решениями, отраженными в документах из п.3.2.1. настоящего Задания	На данном подэтапе проводятся следующие работы: разработка пояснительной записки к техническому проекту путем адаптации типового технического проекта СЗПДн, описанного в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001 (адаптация производится в соответствии с логикой применений мер защиты, которая описана в документе «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001); разработка режимов работы и параметров конфигурации СрЗИ, необходимых для удовлетворения требованиям по настройке компонент СЗПДн, которая отражены в документа «Типовое техническое решение СЗПДн. Пояснительная записка», ИРАО.ТТП.2020.007.ПЗ.001; разработка схемы комплекса технических средств путем адаптации документа «Типовое техническое решение СЗПДн. Схема комплекса технических средств», ИРАО.ТТП.2020.008.КТС.001; разработка ведомости оборудования и материалов путем адаптации документа «Типовое техническое решение СЗПДн. Ведомость оборудования и материалов», ИРАО.ТТП.2020.009.ВО.001 (при адаптации ведомости оборудования и материалов необходимо учесть имеющиеся в Типовом ДО СрЗИ, а так же учесть необходимость закупки инженерно-технического оборудования и материалов, необходимых для внедрения СЗПДн); разработка плана расположения оборудования;	Техно-рабочий проект СЗПДн Общества, включая: Ведомость технорабочего проекта. Пояснительная записка к техно-рабочему проекту (включая описание и характеристики защищаемой системы, требования и обоснование численности и ролей персонала, подтверждается парирование выявленных угроз и действий нарушителей, функциональные схемы по каждой подсистеме в составе СЗПДн, определение режимов работы и параметров конфигурации СрЗИ, описание отказоустойчивости/резервирования СЗПДн, описание режимов функционирования СЗПДн); Схема комплекса технических средств; Ведомость оборудования и материалов; Планы расположения	



		<p>разработка чертежа установки технических средств;  разработка паспорта СЗПДн Общества;  разработка технического паспорта на СрЗИ ИСПДн;  разработка сетевой матрицы доступа;  разработка схемы сети уровня L2 и L3;  разработка таблицы соединений и подключений.</p>	<p>оборудования;  Чертежи установки технических средств;  Паспорт СЗПДн;  Технический паспорт на СрЗИ ИСПДн;  Сетевая матрица доступа;  Схема сети уровня L2 и L3;  Таблица соединений и подключений.</p>	
4.	Проведение пуско-наладочных работы СЗПДн		<p>План проведение пуско-наладочных работ СрЗИ СЗПДн на внедряемые в рамках настоящего ТЗ подсистемы.  Акт установки средств защиты информации на объекте информатизации  Программа и методика испытаний на внедряемые в рамках настоящего ТЗ подсистемы</p>	
4.1.	Пуско-наладочные работы СрЗИ СЗПДн	<p>В рамках данного подэтапа Исполнитель осуществляет следующие работы:  разработка плана пуско-наладочных работ СрЗИ СЗПДн;  внедрение Подсистемы защиты среды виртуализации, реализованной с использованием встроенных механизмов среды виртуализации;  внедрение Подсистемы защиты автоматизированных рабочих мест пользователей, реализованной с использованием встроенных механизмов ОС;  внедрение подсистемы сбора и анализа событий безопасности, представленной в виде решения MaxPatrol SIEM;  внедрение подсистемы защиты от атак 0 дня  Работы по монтажу и коммутации оборудования СЗПДн выполняются Заказчиком.  Работы по монтажу инженерно-технического оборудования и прокладки необходимых кабельных каналов в соответствии со спецификацией, выполняются Заказчиком.  По окончании пуско-наладочных работ Исполнитель подготавливает Акт установки средств защиты информации на объекте информатизации.</p>	<p>План проведение пуско-наладочных работ СрЗИ СЗПДн.  Акт установки средств защиты информации на объекте информатизации</p>	



4.2.	Разработка Программы и методики испытаний	На данном подэтапе проводится разработка, согласование и утверждение документа «Программа и методика испытаний». Программа и методика испытаний должна включать в себе: методику проведения испытаний; проект Протокола предварительных испытаний; проект Журнала опытной эксплуатации; проект Протокола приемочных испытаний.	Программа и методика испытаний	
5.	Предварительные испытания		Протокол предварительных испытаний Проект Акта о приемке в опытную эксплуатацию СЗПДн	
5.1.	Проведение предварительных испытаний	На данном подэтапе Исполнитель совместно с Заказчиком в составе комиссии, собранной на основании приказа Заказчика, производят предварительные испытания СЗПДн в соответствии с документом «Программа и методика испытаний». Во время проведения предварительных испытаний оформляется протокол предварительных испытаний, который подписывается членами комиссии. На данном подэтапе Исполнитель подготавливает проект Акта о приемке в опытную эксплуатацию СЗПДн. По окончании предварительных испытаний и устранение всех возникших замечаний Заказчик подписывает Акт о приемке в опытную эксплуатацию СЗПДн.	Протокол предварительных испытаний Проект Акта о приемке в опытную эксплуатацию	
6.	Опытная эксплуатация		Журнал опытной эксплуатации Проект Акта о завершении опытной эксплуатации и допуске СЗПДн к приемочным испытаниям.	
6.1.	Проведение опытной эксплуатации	На данном подэтапе Заказчик осуществляет опытную эксплуатацию СЗПДн, а исполнитель осуществляет исправление возникающих замечаний и сбоев в работе компонент СЗПДн. Все замечания, сбои и внесенные изменения фиксируются в Журнале опытной эксплуатации. Опытная эксплуатация проводится не менее 1-ого месяца. По результатам опытной эксплуатации принимается решение о возможности (невозможности) предъявления СЗПДн на приемочные испытания. Опытная эксплуатация завершается оформлением акта о завершении опытной эксплуатации и допуске СЗПДн к приемочным испытаниям.	Журнал опытной эксплуатации Проект Акта о завершении опытной эксплуатации и допуске СЗПДн к приемочным испытаниям.	
7.	Приемочные испытания		Протокол приемочных испытаний Проект Акта о приемке в	



			промышленную эксплуатацию СЗПДн	
7.1.	Проведение приемочных испытаний	<p>На данном подэтапе Исполнитель совместно с Заказчиком в составе комиссии, собранной на основании приказа Заказчика, производят приемочные испытания СЗПДн в соответствии с документом «Программа и методика испытаний».</p> <p>Во время проведения приемочных испытаний оформляется протокол приемочных испытаний, который подписывается членами комиссии.</p> <p>На данном подэтапе Исполнитель подготавливает проект Акта о приемке в промышленную эксплуатацию СЗПДн.</p> <p>По окончании приемочных испытаний и устранение всех возникших замечаний Заказчик подписывает Акт о приемке в промышленную эксплуатацию СЗПДн.</p>	<p>Протокол приемочных испытаний</p> <p>Проект Акта о приемке в промышленную эксплуатацию</p>	



## 7. Порядок контроля и приемки работ

### 7.1. Требования к приемке работ по стадиям

По окончании этапов, предусмотренных разделе 6 настоящего Задания, Заказчиком должна производиться приемка результатов работ этапа.

Завершение работ должно оформляться актом сдачи-приемки работ, утверждаемым уполномоченными представителями Сторон в соответствии с требованиями Договора.

Документы – результаты этапов к актам сдачи-приемки работ должны предоставляться согласованными и утвержденными. Перечень утверждающих и согласующих лиц определяется в рабочем порядке в рамках зон ответственности Заказчика и Исполнителя.

## 8. Требования к документированию

### 8.1. Требования к составу документации

Требования к перечню и составу документации приведены в разделе 6 настоящего Задания.

### 8.2. Требования к оформлению документации

Все документы проекта должны формироваться строго на соответствующих этапах проекта.

Оформление документов на СЗПДн должно соответствовать требованиям ГОСТ 34.201-89; ГОСТ 34.603-92.

Документы готовятся в стандартных офисных приложениях Microsoft Office (Word, Excel, Project, Visio) и в печатном виде.

На приемку предоставляются документы в формате, определенном п. **Ошибка! Источник ссылки не найден.** в доступном для редактирования режиме.

В ходе согласования документов необходимо использовать Комментарии для описания замечания и обоснования замечания. При внесении изменений по замечаниям использовать режим TrackChange в тех приложениях, где это возможно. По непринятым и неотработанным замечаниям использовать Комментарии для приведения обоснования отказа.

Результирующие документы должны быть предоставлены в двух вариантах:

- в электронном виде – в форме файлов приложений, определенных в п. **Ошибка! Источник ссылки не найден.**, записанных на оптическом носителе (CD-ROM) в одном экземпляре;

- в печатном виде – в форме сброшюрованных книг.

Документы в печатном виде должны быть представлены в двух экземплярах:

- для Заказчика;
- для Исполнителя.

### 8.3. Виды, состав, объем и методы испытаний

В таблице **Ошибка! Источник ссылки не найден.** приведен краткий перечень и этапность проведения работ. Подробно сами работы описаны в разделе «7. **Ошибка! Источник ссылки не найден.**».

Таблица 2 – Этапность выполнения работ

	Наименование работ
1	Пуско-наладочные работы
2	Предварительные испытания
3	Опытная эксплуатация
4	Приемочные испытания

#### 8.3.1. Пуско-наладочные работы

Пуско-наладочные работы проводятся на технологических площадках Общества, перечень которых приведен в приложении 1 «Перечень технологических площадок Общества» к настоящему Заданию.

Работы по настройке централизованных компонент СЗПДн Общества, расположенных в ЦОД БЦ «Луч» по адресу: г. Москва, ул. Большая Пироговская, д. 27 осуществляются Заказчиком.

Работы производятся в соответствии с документацией перечисленной в разделе 5.1. настоящего Заданию.

До начала проведения пуско-наладочных работ Исполнитель разрабатывает и согласует с Заказчиком «План проведение пуско-наладочных работ СрЗИ СЗПДн».

План проведения пуско-наладочных работ СрЗИ СЗПДн должен включать в себя порядок и график производства работ.





Порядок проведения работ должен описывать последовательность проведения работ, ответственных за выполнение работ, зависимости в работах по созданию СЗПДн с учетом работ, осуществляемых Заказчиком по подготовке объекта автоматизации к вводу СЗПДн в действие (п. 5.2.настоящего Заданию).

График производства работ должен включать в себя календарный план-график работ по созданию СЗПДн с учетом работ, осуществляемых Заказчиком по подготовке объекта автоматизации к вводу СЗПДн в действие.

### 8.3.2. Предварительные испытания

Порядок контроля и приемки работ по внедрению СЗПДн, виды, состав, объем и методы испытаний подсистем и их составных частей, перечень организаций, участвующих в приемке работ, сроки и место приемки должны быть определены в документе «Программа и методика испытаний».

Документ «Программа и методика испытаний» должен содержать перечни конкретных проверок, которые следует осуществлять при испытаниях для подтверждения выполнения требований настоящего Задания, со ссылками на соответствующие методики испытаний.

Перечень проверок, подлежащих включению в документ «Программа и методика испытаний», должен включать:

- соответствие СЗПДн настоящему Заданию;
- комплектность СЗПДн;
- степень выполнения требований функционального назначения СЗПДн.

Документ «Программа и методика испытаний» должен включать в себя следующие разделы:

- объект испытаний;
- цель испытаний;
- общие положения;
- объем испытаний;
- условия и порядок проведения испытаний;
- методика проведения испытаний.

Результаты предварительных испытаний оформляются протоколом предварительных испытаний, который подписывается членами комиссии и утверждается лицом, определённым приказом Исполнителя. По результатам предварительных испытаний составляется акт о приемке СЗПДн в опытную эксплуатацию. Форма акта и протокола должны быть подготовлены Исполнителем в виде приложения к документу «Программа и методика испытаний».

В ходе предварительных испытаний СЗПДн члены комиссии должны удостовериться в соответствии предъявленных результатов работ техническому решению, описанному СЗПДн Общества.

В случае неготовности СЗПДн к опытной эксплуатации в протоколе предварительных испытаний фиксируются замечания, и назначается дата проведения повторных предварительных испытаний.

### 8.3.3. Опытная эксплуатация

В рамках опытной эксплуатации ведется Журнал опытной эксплуатации, в который заносятся сведения о продолжительности функционирования СЗПДн, отказах, сбоях, аварийных ситуациях, изменениях параметров компонент СЗПДн, проводимых корректировках документации и программных средств, наладке технических средств. Сведения фиксируют в журнале с указанием даты и ответственного лица.

В случае выявления во время опытной эксплуатации СЗПДн отказа или сбоя в работе ИСПДн производятся изменения в конфигурации СЗПДн, позволяющее нейтрализовать произошедший отказ или сбой ИСПДн, указанные изменения вносятся в журнал опытной эксплуатации с указанием комментария о том, что изменения были внесены в результате отказа или сбоя ИСПДн.

Критичность замечаний к подсистеме должны классифицироваться по следующим признакам:

- блокирующие – замечания (ошибки), препятствующие выполнению основных штатных функций СЗПДн;
- критичные – замечания (ошибки), значительно затрудняющие выполнение основных штатных процедур СЗПДн;
- важные – замечания (ошибки), не влияющие на выполнение основных штатных процедур СЗПДн, но оказывающие значительные неудобства пользователям;
- обычные – замечания (ошибки), не влияющие на выполнение основных штатных процедур СЗПДн, устранение которых повышает удобство и производительность (эффективность) компонентов СЗПДн.



Обновление программного обеспечения, устраняющее блокирующее замечание, проводится немедленно после устранения ошибки. Остальные обновления могут группироваться для обновления в согласованные Заказчиком и Исполнителем сроки. Устранение замечаний пользователей к работе СЗПДн должно также фиксироваться в журнале опытной эксплуатации.

В случае неготовности СЗПДн к проведению приемочных испытаний в протоколе опытной эксплуатации фиксируются критические (блокирующие) замечания и рекомендация о продлении опытной эксплуатации до определенного срока, обеспечивающего устранение указанных замечаний.

По результатам опытной эксплуатации принимают решение о возможности (или невозможности) предъявления СЗПДн на приемочные испытания.

#### 8.3.4. Приемочные испытания

Приемочные испытания проводятся с целью определения соответствия СЗПДн требованиям настоящего Задания и решения вопроса о возможности приёмки СЗПДн в промышленную эксплуатацию.

Приёмочные испытания проводятся в соответствии с документом «Программа и методика испытаний» на технических средствах СЗПДн в сроки, установленные распоряжением комиссии, в состав которой входят представители Заказчика и Исполнителя.

По результатам приемочных испытаний оформляется Протокол приемочных испытаний. При наличии существенных замечаний после их устранения приемочные испытания проводятся повторно. По результатам приемочных испытаний составляется акт о приемке СЗПДн в промышленную эксплуатацию.

Решение о необходимости проведения дополнительных испытаний, составе и цели проведения дополнительных испытаний, принимается в случае не прохождения испытаний или приемки СЗПДн в промышленную эксплуатацию.

#### 8.3.5. Общие требования к приемке работ

Контроль и приемку внедряемой СЗПДн и актуализированного комплекта документации осуществляют:

- Заказчик;
- Исполнитель.

По окончании каждого из этапов, предусмотренных в разделе **Ошибка! Источник ссылки не найден.** настоящего Задания, Заказчиком должна производиться приемка результатов работ этапа.

Завершение работ должно оформляться актом сдачи-приемки работ, утверждаемым уполномоченными представителями Сторон в соответствии с требованиями Договора.

Документы – результаты этапов к актам сдачи-приемки работ должны предоставляться согласованными и утвержденными. Перечень утверждающих и согласующих лиц определяется в рабочем порядке в рамках зон ответственности Заказчика и Исполнителя.

#### Поставщик:

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

#### Покупатель:

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.



Перечень технологических площадок Общества

№	Наименование ИСПДн	Уровень защищенности	Владелец
1.	Информационная система управления сбытом электроэнергии бытовым потребителям (ИСУСЭ БП)	УЗ-3	Общество
2.	Информационно-аналитическая система (ИАС)	УЗ-3	Общество
3.	Индивидуальный кабинет управления счетами (ИКУС)	УЗ-3	Общество
4.	Единая Биллинговая Система для Расчетов с Юридическими Лицами (ЕБ ЮЛ)	УЗ-4	Общество
5.	Единая Биллинговая Система для Расчетов с Юридическими Лицами в импортозамещенной конфигурации (ЕБ ЮЛ ИК)	УЗ-4	Общество
6.	CRM Юридических лиц	УЗ-4	Общество
7.	Сигма. Электронный архив	Не определен	Общество
8.	СКУД	УЗ-4	Общество

**Поставщик:**  
Заместитель генерального директора  
  
\_\_\_\_\_ Пестунов А.В.

**Покупатель:**  
Директор по информационным технологиям  
  
\_\_\_\_\_ Белокуров М.И.



Перечень мер защиты для нейтрализации актуальных УБИ для централизованных ИСПДн

№ УБИ	Наименование актуальной УБИ	Мера защиты (приказ № 21 ФСТЭК России)	Функции подсистемы защиты СЗПДн	Подсистема защиты СЗПДн
УБИ.006	Угроза внедрения кода или данных	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов операционной системы (далее – ОС)	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
			Анализ почтового трафика на предмет наличия вредоносных вложений и нежелательных электронных писем, ссылок на опасные сайты Отправка на проверку вложенных в электронные письма файлы в подсистему защиты от атак 0 дня Наличие механизмов проверки репутации отправителя, протокола, содержимого письма, репутации IP-адреса домена	Подсистема защиты электронной почты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	Подсистема антивирусной защиты
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
			АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме,



			достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка») Отправка на проверку файлов в подсистему защиты от атак 0 дня, передаваемых по протоколам HTTP(s), (s)FTP, IM	Подсистема межсетевого экранирования и обнаружения вторжений
			Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		ЗИС.11	Фильтрация сетевых пакетов с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов (антиспуфинг)	Подсистема межсетевого экранирования и обнаружения вторжений
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	
УБИ.008	Угроза восстановления аутентификационной информации	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Организационные меры
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам	Подсистема анализа защищенности





			Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		АНЗ.5	Контроль правил генерации и смены паролей пользователей	
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS			Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.012	Угроза деструктивного изменения конфигурации/ среды окружения программ	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.7	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	Подсистема защиты среды виртуализации
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по	Подсистема анализа защищенности



			сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещениях и сооружениях, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещениях и сооружениях, в которых они установлены	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.014	Угроза длительного удержания вычислительных ресурсов	АНЗ.1	Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Сбор сведений о конфигурации	Подсистема анализа защищенности



	пользователями		программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		АНЗ.3	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам	
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.018	Угроза загрузки нештатной ОС	УПД.2	Организационные меры	Организационные меры
УБИ.019	Угроза заражения DNS-кеша	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений



		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.022	Угроза избыточного выделения оперативной памяти	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.023	Угроза изменения компонентов системы	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
		ОЦЛ.1	Возможность контроля целостности	Подсистема защиты



			программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	автоматизированных рабочих мест пользователей
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	Подсистема анализа защищенности
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
УБИ.030	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.5	Реализация настроек сложности паролей и механизм генерации пароля, соответствующего настройкам	Подсистема защиты автоматизированных рабочих мест пользователей
			Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Выявление учетных записей с паролями, содержащимися в справочниках, задаваемых администратором в настройках сканирования (словарными паролями)	Подсистема анализа защищенности
УБИ.031	Угроза использования	УПД.2	Реализация механизма разграничений	Подсистема защиты





	механизмов авторизации для повышения привилегий		прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
УБИ.041	Угроза межсайтового скриптинга	АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов	Подсистема защиты автоматизированных рабочих мест пользователей



			ОС	
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности и защита от НСД компонентов СЗИ	
УБИ.049	Угроза нарушения целостности данных кэша	СОВ.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами	Подсистема защиты от атак нулевого дня



			подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.053	Угроза невозможности управления правами пользователей BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности и защита от НСД компонентов СЗИ	
УБИ.062	Угроза некорректного использования	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме	Подсистема антивирусной



	прозрачного прокси-сервера за счёт плагинів браузера		постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.067	Угроза неправомерного ознакомления защищаемой информацией с	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
УБИ.069	Угроза неправомерных действий в каналах связи	ЗИС.11	Фильтрация сетевых пакетов с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов (антиспуфинг)	Подсистема межсетевого экранирования и обнаружения вторжений
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры	



			Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	
		ИАФ.1	Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	ЗНИ.8	Очистка остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктуры Фильтрация сетевого трафика при	Подсистема межсетевого экранирования и обнаружения вторжений





			взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации	



			виртуальных машин и их доверенная загрузка	
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.088	Угроза несанкционированного копирования защищаемой информации	ЗНИ. 2	Разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации



УБИ.089	Угроза несанкционированного редактирования реестра	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ.091	Угроза несанкционированного удаления защищаемой информации	УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.093	Угроза несанкционированного управления буфером	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		СОВ.1 СОВ.2	Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых	Подсистема анализа защищенности



			протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	
УБИ.099	Угроза обнаружения хостов	СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.103	Угроза определения типов объектов защиты	ИАФ.1	Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH	Подсистема межсетевого экранирования и обнаружения вторжений
		УПД.3	Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	
УБИ.104	Угроза определения топологии вычислительной сети	РСБ.3	Регистрация фактов установления сетевых сессий Регистрация событий фильтрации трафика и передача в компонент централизованного сбора событий действий администратора за сеанс Регистрация событий обнаружения опасной сетевой активности	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей	Подсистема анализа защищенности



			программного обеспечения сканируемого узла	
УБИ.108	Угроза ошибки обновления гипервизора	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		ЗСВ.3	Регистрация событий, связанных с информационной безопасностью	
		ЗСВ.7	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
УБИ.121	Угроза повреждения системного реестра	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также	Подсистема защиты автоматизированных рабочих мест пользователей





			контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
УБИ.123	Угроза подбора пароля BIOS	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.124	Угроза подделки записей журнала регистрации событий	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.128	Угроза подмены доверенного пользователя	ИАФ.1	Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗИС.11	Фильтрация сетевых пакетов с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов (антиспуфинг)	
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов,	



			служащих для диагностики и управления работой сетевых устройств	
УБИ.129	Угроза подмены резервной копии ПО BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационные меры
УБИ.130	Угроза подмены содержимого сетевых ресурсов	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		ЗИС.11	Фильтрация сетевых пакетов с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов (антиспуфинг)	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	
УБИ.144	Угроза программного сброса пароля BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе	Подсистема защиты автоматизированных рабочих мест пользователей



			и блокировку входа в ОС при выявлении изменений	Организационные меры
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений
		COB.1, COB.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.152	Угроза удаления аутентификационной информации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.153	Угроза усиления	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений



	воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов		организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
		COB.1, COB.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.155	Угроза утраты вычислительных ресурсов	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей	Подсистема межсетевого экранирования и обнаружения вторжений
			Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
		COB.1, COB.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.156	Угроза утраты носителей информации	ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны	Организационные меры
		ЗНИ.4	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.158	Угроза форматирования носителей информации	ЗНИ. 2	Управление доступом к машинным носителям персональных данных	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.5	Назначение минимально необходимых	Организационные



			прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	меры
УБИ.159	Угроза «форсированного веб-браузинга»	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам,	Организационные меры



			обеспечивающим функционирование информационной системы	
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		COB.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак. Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	УПД.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.170	Угроза неправомерного шифрования информации	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		COB.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак. Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.171	Угроза скрытного включения вычислительного устройства в состав	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и	Подсистема антивирусной защиты





	бот-сети		сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		COB.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
УБИ.172	Угроза распространения «почтовых червей»	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	Подсистема защиты от атак нулевого дня
		COB.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	
		AB3.1	Анализ почтового трафика на предмет наличия вредоносных вложений и нежелательных электронных писем, ссылок на опасные сайты	Подсистема защиты электронной почты
УБИ.173	Угроза «спама» веб-сервера	ОЦЛ.4	Анализ почтового трафика на предмет наличия вредоносных вложений и нежелательных электронных писем, ссылок на опасные сайты Наличие механизмов проверки репутации отправителя, протокола, содержимого письма, репутации IP-адреса домена	Подсистема защиты электронной почты
УБИ.174	Угроза «фарминга»	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	Подсистема межсетевого экранирования
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей	



				обнаружения вторжений
		СОВ.1	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДН на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка») Регистрация событий обнаружения опасной сетевой активности	Подсистема межсетевого экранирования и обнаружения вторжений Подсистема защиты web-приложений
УБИ.175	Угроза «фишинга»	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОЦЛ.4	Анализ почтового трафика на предмет наличия вредоносных вложений и нежелательных электронных писем, ссылок на опасные сайты Отправка на проверку вложенных в электронные письма файлы в подсистему защиты от атак 0 дня Наличие механизмов проверки репутации отправителя, протокола, содержимого письма, репутации IP-адреса домена	Подсистема защиты электронной почты
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных	Организационные меры
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.179	Угроза несанкционированной модификации защищаемой информации	ЗНИ.2	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати	



			документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.185	Угроза несанкционированного изменения параметров настройки СрЗИ	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		СОВ.1, АВ3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня



		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив ПО	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.192	Угроза использования уязвимых версий ПО	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае вторжений	Подсистема межсетевого экранирования и обнаружения вторжений



			обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры	
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	Подсистема анализа защищенности
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.209	Угроза несанкционированного	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме	Подсистема антивирусной



	доступа к защищаемой памяти ядра процессора		постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей,	





			обусловленных ошибками конфигурации	
--	--	--	-------------------------------------	--

Перечень мер защиты для нейтрализации актуальных УБИ для Локальных ИСПДн

№ УБИ	Наименование актуальной УБИ	Мера защиты (приказ № 21 ФСТЭК России)	Функции подсистемы защиты СЗПДн	Подсистема защиты СЗПДн
УБИ.008	Угроза восстановления аутентификационной информации	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Организационные меры
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		АНЗ.5	Контроль правил генерации и смены паролей пользователей	
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация	Подсистема анализа защищенности



			<p>уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов</p> <p>Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла</p> <p>Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений</p>	
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.012	Угроза деструктивного изменения конфигурации/ среды окружения программ	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.7	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	Подсистема защиты среды виртуализации
		АНЗ.1	<p>Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам</p> <p>Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам</p> <p>Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов</p> <p>Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла</p> <p>Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений</p>	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей



УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	АНЗ.1	Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	Подсистема анализа защищенности
		АНЗ.3	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам	
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.018	Угроза загрузки нештатной ОС	УПД.2	Организационные меры	Организационные меры
УБИ.022	Угроза избыточного выделения оперативной памяти	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и	Подсистема антивирусной защиты



			сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.023	Угроза изменения компонентов системы	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	Подсистема анализа защищенности
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	



УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
УБИ.030	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.5	Реализация настроек сложности паролей и механизм генерации пароля, соответствующего настройкам	Подсистема защиты автоматизированных рабочих мест пользователей
			Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Выявление учетных записей с паролями, содержащимися в справочниках, задаваемых администратором в настройках сканирования (словарными паролями)	Подсистема анализа защищенности
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме,	



			достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентов ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД	





			Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности и защита от НСД компонентов СЗИ	
УБИ.049	Угроза нарушения целостности данных кэша	СОВ.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.053	Угроза невозможности управления правами пользователей BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений



		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности и защита от НСД компонентов СЗИ	
УБИ.067	Угроза неправомерного ознакомления защищаемой информацией с	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
	Угроза несанкционированного восстановления удалённой защищаемой информации	ЗНИ.8	Очистка остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов	Подсистема защиты автоматизированных рабочих мест пользователей
	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.074	Угроза несанкционированного доступа к	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати	Подсистема защиты автоматизированных рабочих мест



	аутентификационной информации		документов независимого от механизмов ОС	пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	Подсистема защиты среды виртуализации
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	



УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
		ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		ЗСВ.3	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Защита средств управления виртуальной инфраструктурой от НСД Защита гипервизоров от НСД Мандатный принцип контроля доступа	
		УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов	Подсистема защиты автоматизированных рабочих мест пользователей



			механизмов ОС	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.088	Угроза несанкционированного копирования защищаемой информации	ЗНИ. 2	Разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	Подсистема криптографической защиты информации
УБИ.089	Угроза несанкционированного редактирования реестра	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ.091	Угроза несанкционированного удаления защищаемой информации	УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.093	Угроза несанкционированного управления буфером	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей



			Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	автоматизированных рабочих мест пользователей
		COB.1 COB.2	Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.103	Угроза определения типов объектов защиты	ИАФ.1	Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH	Подсистема межсетевого экранирования и обнаружения вторжений
		УПД.3	Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	
УБИ.108	Угроза ошибки обновления гипервизора	ЗСВ.1	Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности	Подсистема защиты среды виртуализации
		ЗСВ.2	Мандатный принцип контроля доступа	
		ЗСВ.3	Регистрация событий, связанных с информационной безопасностью	
		ЗСВ.7	Контроль целостности конфигурации виртуальных машин и их доверенная загрузка	
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей





УБИ.121	Угроза повреждения системного реестра	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.123	Угроза подбора пароля BIOS	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.124	Угроза подделки записей журнала регистрации событий	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.129	Угроза подмены резервной копии ПО BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1	Возможность создания для пользователя	



		ОПС.2 ОПС.3	замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационные меры
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	
УБИ.144	Угроза программного сброса пароля BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационные меры
УБИ.152	Угроза удаления аутентификационной информации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры



			обеспечивающих функционирование информационной системы	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.155	Угроза утраты вычислительных ресурсов	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей	Подсистема межсетевого экранирования и обнаружения вторжений
			Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
УБИ.156	Угроза утраты носителей информации	ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны	Организационные меры
		ЗНИ.4	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический	Организационные меры



			доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	
УБИ.158	Угроза форматирования носителей информации	ЗНИ.2	Управление доступом к машинным носителям персональных данных	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	



		СОВ.1, АВЗ.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных	Организационные меры
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.179	Угроза несанкционированной модификации защищаемой информации	ЗНИ.2	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	
УБИ.185	Угроза несанкционированного изменения параметров настройки СрЗИ	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса,	Подсистема межсетевого экранирования и обнаружения вторжений



			локальной консоли управления и удаленной текстовой консоли по протоколу SSH Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		СОВ.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив ПО	AB3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		AB3.2	Автоматическое обновление	





			антивирусных баз и программных модулей по расписанию	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.192	Угроза использования уязвимых версий ПО	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности



			Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры	
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1	Анализ сетевой активности	



			защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	



Перечень мер защиты для нейтрализации актуальных УБИ для ИСПДн Общества

№ УБИ	Наименование актуальной УБИ	Мера защиты (приказ № 21 ФСТЭК России)	Функции подсистемы защиты СЗПДн	Подсистема защиты СЗПДн
УБИ.008	Угроза восстановления аутентификационной информации	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Организационные меры
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		АНЗ.5	Контроль правил генерации и смены паролей пользователей	
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ.012	Угроза деструктивного изменения конфигурации/ среды	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей



	окружения программ	АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	АНЗ.1	Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	Подсистема анализа защищенности
		АНЗ.3	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам	
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	
УБИ.015	Угроза доступа к защищаемым файлам с использованием	УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей



	ем обходного пути			
УБИ .018	Угроза загрузки нештатной ОС	УПД.2	Организационные меры	Организационные меры
УБИ .022	Угроза избыточного выделения оперативной памяти	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		АН3.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АН3.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ .023	Угроза изменения компонентов системы	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		АН3.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла	Подсистема анализа защищенности
		АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ .027	Угроза искажения вводимой и выводимой на периферийные устройства информации	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ .028	Угроза использования альтернативных путей доступа к ресурсам	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .030	Угроза использования	УПД.2	Контроль входа пользователей в систему	Подсистема защиты





	я информации идентификации/ аутентификации, заданной по умолчанию			автоматизированных рабочих мест пользователей
		АНЗ.5	Реализация настроек сложности паролей и механизм генерации пароля, соответствующего настройкам	Подсистема защиты автоматизированных рабочих мест пользователей
			Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Выявление учетных записей с паролями, содержащимися в справочниках, задаваемых администратором в настройках сканирования (словарными паролями)	Подсистема анализа защищенности
УБИ .031	Угроза использования механизмов авторизации для повышения привилегий	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		АНЗ.1	Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла	Подсистема анализа защищенности
		АНЗ.3	Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	
УБИ .034	Угроза использования слабостей протоколов сетевого/локального обмена данными			
УБИ .045	Угроза нарушения изоляции среды исполнения BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ .049	Угроза нарушения целостности	СОВ.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак	Подсистема защиты от атак



	данных кэша		Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ .053	Угроза невозможности управления правами пользователей BIOS	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ .067	Угроза неправомерного ознакомления с защищаемой информацией	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ .071	Угроза несанкционированного восстановления удалённой защищаемой информации	ЗНИ.8	Очистка остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов	
УБИ .072	Угроза несанкционированного	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде	Подсистема защиты автоматизированных рабочих мест пользователей



	выключения или обхода механизма защиты от записи в BIOS		администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	ных рабочих мест пользователей
УБИ .074	Угроза несанкционированного доступа к аутентификационной информации	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
УБИ .084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ .086	Угроза несанкционированного изменения аутентификационной информации	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .087	Угроза несанкционированного использования привилегированных функций BIOS	УПД.2	Контроль входа пользователей в систему	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .088	Угроза несанкционированного копирования защищаемой	ЗНИ. 2	Разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	



	информации	ЗИС.3	Защита информации от ее модификации и перехвата при ее передаче через каналы связи, пролегающие за пределами контролируемой зоны	
УБИ .089	Угроза несанкционированного редактирования реестра	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ .090	Угроза несанкционированного создания учётной записи пользователя	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
УБИ .091	Угроза несанкционированного удаления защищаемой информации	УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .093	Угроза несанкционированного управления буфером	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.2	Контроль входа пользователей в систему Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		СОВ.1 СОВ.2	Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
УБИ .100	Угроза обхода некорректно настроенных механизмов аутентификации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ .115	Угроза перехвата вводимой и выводимой на периферийные устройства	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты



	информации	AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .121	Угроза повреждения системного реестра	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .123	Угроза подбора пароля BIOS	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .124	Угроза подделки записей журнала регистрации событий	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ .129	Угроза подмены резервной копии ПО BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	





			администраторов и лиц, обеспечивающих функционирование информационной системы	е меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационны е меры
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационны е меры
УБИ .140	Угроза приведения системы в состояние «отказ в обслуживании»	УПД.3	Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	
УБИ .144	Угроза программного сброса пароля BIOS	ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационны е меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационны е меры
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационны е меры
УБИ .152	Угроза удаления аутентификационной информации	ИАФ.1	Идентификация и проверка подлинности пользователей при входе в операционную систему	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационны е меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационны е меры
УБИ .155	Угроза утраты вычислительных ресурсов	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей	Подсистема межсетевого экранирования и обнаружения вторжений
			Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема защиты web-приложений Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1, СОВ.2	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования	Подсистема защиты web-приложений





			производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	приложений Подсистема межсетевого экранирования и обнаружения вторжений
УБИ .156	Угроза утраты носителей информации	ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны	Организационные меры
		ЗНИ.4	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ .158	Угроза форматирования носителей информации	ЗНИ. 2	Управление доступом к машинным носителям персональных данных	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ .160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	Организационные меры
		ЗТС.3	Контроль и управление физическим доступом к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Организационные меры
УБИ .162	Угроза эксплуатации цифровой подписи программного кода	УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизированных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ	Угроза	АВЗ.1	Обнаружение и уничтожение вредоносных программ в	Подсистема



.167	заражения компьютера при посещении неблагонадежных сайтов		режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	антивирусной защиты
		AB3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		СОВ.1, AB3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных	Организационные меры
УБИ .178	Угроза несанкционированного использования системных и сетевых утилит	ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
УБИ .179	Угроза несанкционированной модификации защищаемой информации	ЗНИ.2	Шифрование данных, хранящихся в криптоконтейнерах	Подсистема защиты автоматизированных рабочих мест пользователей
		ОЦЛ.1	Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию, а также контроль целостности файлов при доступе и блокировку входа в ОС при выявлении изменений	
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Организационные меры
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	
УБИ .185	Угроза несанкционированного изменения параметров настройки СрЗИ	УПД.3	Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗИДн с интерфейсами управления компонентом СЗИДн Идентификация, аутентификация и учет администраторов подсистемы при доступе к ПО компонентов подсистемы посредством WEB интерфейса, локальной консоли управления и удаленной текстовой консоли по протоколу SSH Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	Подсистема межсетевого экранирования и обнаружения вторжений
		ОПС.1	Возможность создания для пользователя замкнутой	Подсистема



		ОПС.2 ОПС.3	программной среды	защиты автоматизирован ных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационны е меры
УБИ .186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		СОВ.1, АВ3.1	Выполнение эмуляции кода в изолированной защищенной среде для раскрытия поведения и обнаружения сложных угроз и целенаправленных атак Возможность интеграции с компонентами подсистемы межсетевого экранирования и обнаружения вторжений и подсистемы защиты электронной почты в части получения контента на анализ	Подсистема защиты от атак нулевого дня
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	Подсистема защиты автоматизирован ных рабочих мест пользователей
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	
УБИ .191	Угроза внедрения вредоносного кода в дистрибутив ПО	АВ3.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВ3.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизирован ных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.4	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационны е меры
УБИ .192	Угроза использовани я уязвимых версий ПО	УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонент СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений	Подсистема межсетевого экранирования и обнаружения вторжений



			эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты Фильтрация служебных протоколов, служащих для диагностики и управления работой сетевых устройств	
		СОВ.1	Анализ сетевой активности защищаемых сегментов с использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	Подсистема межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры	
УБИ .208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		ОПС.1 ОПС.2 ОПС.3	Возможность создания для пользователя замкнутой программной среды	Подсистема защиты автоматизированных рабочих мест пользователей
		УПД.2	Реализация механизма разграничений прав доступа к объектам файловой системы, к запуску программ и к печати документов независимого от механизмов ОС	
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Организационные меры
УБИ .209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	АВЗ.1	Обнаружение и уничтожение вредоносных программ в режиме постоянной защиты (проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов) и проверки по требованию, а также проверка мобильного исполняемого кода, блокировка опасных скриптов	Подсистема антивирусной защиты
		АВЗ.2	Автоматическое обновление антивирусных баз и программных модулей по расписанию	
		УПД.3	Фильтрация сетевого трафика при взаимодействии серверных компонентов ИСПДн с АРМ пользователей Фильтрация сетевого трафика при взаимодействии администраторов ИТ инфраструктуры с интерфейсами управления компонентами ИТ инфраструктуры Фильтрация сетевого трафика при взаимодействии администраторов СЗПДн с интерфейсами управления компонентом СЗПДн Инспекция информационных потоков, организуемых с серверами защищаемых ИСПДн на уровне приложений эталонной модели OSI на предмет предотвращения вторжений с использованием различных профилей защиты	Подсистема межсетевого экранирования и обнаружения вторжений
		СОВ.1	Анализ сетевой активности защищаемых сегментов с	



			использованием баз сигнатур, предоставленных производителем оборудования Автоматическое реагирование в случае обнаружения сетевых атак (применение действий «обнаружение» или «блокировка»)	межсетевого экранирования и обнаружения вторжений
		АНЗ.1	Выявление и идентификация узлов, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам Выявление и идентификация портов транспортного уровня сетевых протоколов, доступных в момент сканирования, по протоколам и номерам Выявление и идентификация уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов Сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла Выявление уязвимостей в доступных по протоколу HTTP веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений	Подсистема анализа защищенности
		АНЗ.4	Инвентаризация объектов ИТ-инфраструктуры Сбор сведений о составе программного и аппаратного обеспечения сканируемого узла Сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации	

**Поставщик:**

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

**Покупатель:**

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.



**Форма по раскрытию информации в отношении всей цепочки собственников, включая бенефициаров (в том числе, конечных)**

*Организационно-правовая форма (полностью) «Наименование контрагента»*

*Дата*

№ п/ п	Наименование контрагента (ИНН, вид деятельности)						Информация в отношении всей цепочки собственников, включая бенефициаров (в том числе конечных)								
	ИНН	ОГРН	Наименование краткое	Код ОКВЭД	Фамилия, Имя, Отчество руководителя	Серия и номер документа удостоверяющего личность руководителя	№	ИНН (при наличии)	ОГРН	Наименование / Ф.И.О.	Адрес регистрации	Серия и номер документа, удостоверяющего личность физического лица	Руководитель /участник /бенефициар	Информация о подтверждающих документах (наименование, номера и т.д.)	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1.															

- Контрагент (Поставщик) гарантирует Обществу (Покупателю), что сведения и документы в отношении всей цепочки собственников и руководителей, включая бенефициаров (в том числе конечных), передаваемые Обществу (Покупателю) являются полными, точными и достоверными.
- Контрагент (Поставщик) настоящим выдает согласие и подтверждает получение им всех требуемых в соответствии с действующим законодательством РФ (в том числе о коммерческой тайне и о персональных данных) согласий всех упомянутых в сведениях, заинтересованных или причастных к сведениям лиц на обработку, а также на раскрытие Обществом (Покупателем) полностью или частично представленных сведений компетентным органам государственной власти (в том числе, но, не ограничиваясь, Федеральной налоговой службе РФ, Минэнерго России, Росфинмониторингу, Правительству РФ) и последующую обработку сведений такими органами (далее – Раскрытие). Контрагент (Поставщик) настоящим освобождает Общество (Покупателя) от любой ответственности в связи с Раскрытием, в том числе возмещает Обществу (Покупателю) убытки, понесенные в связи с предъявлением Обществу (Покупателю) претензий, исков и требований любыми третьими лицами, чьи права были или могли быть нарушены таким Раскрытием.

**Подпись уполномоченного лица организации  
печать организации**

**Поставщик:**  
Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

**Покупатель:**  
Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.





**Форма согласия на обработку персональных данных**

**СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, (указать: фамилия имя, отчество, адрес, номер документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе), даю согласие на обработку моих персональных данных (фамилия, имя, отчество, место жительства, ИНН, номер документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе) следующим операторам:

- Акционерному обществу «Петербургская сбытовая компания» (195009, Санкт-Петербург, ул. Михайлова д.11),
- Публичному акционерному обществу «Интер РАО ЕЭС» (119435, г. Москва, ул. Большая Пироговская, д. 27, стр. 2.),
- Обществу с ограниченной ответственностью «Интер РАО - Центр управления закупками» (119435, г. Москва, ул. Б. Пироговская, д. 27. Стр. 3А),
- Правительству Российской Федерации (103274, Москва, Краснопресненская наб., 2),
- Министерству энергетики Российской Федерации (107996 ГСП-6 г. Москва, ул. Щепкина, д.42),
- Федеральной службе по финансовому мониторингу (107450, Москва, К-450, ул. Мясницкая, дом 39, строение 1),
- Федеральной налоговой службе (127381, Москва, Неглинная ул., 23).

Действия по обработке моих персональных данных указанными операторами включают: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), передачу (предоставление доступа) персональных данных компаниям, входящими в Группу «Интер РАО», извлечение, обезличивание, блокирование, удаление, уничтожение.

Любые действия по обработке моих персональных данных допускается осуществлять указанными операторами исключительно в целях выполнения Поручений Председателя Правительства Российской Федерации от 28 декабря 2011 года № ВП-П13-9308, от 5 марта 2012 года № ВП-П24-1269.

Обработка моих персональных данных допускается, как с использованием автоматизированных информационных систем, так и без их использования в объеме, необходимом для цели обработки моих персональных данных.

Настоящее согласие на обработку моих персональных данных действует в течение 1 (одного) года или до его отзыва мною путём направления вышеуказанным операторам письменного уведомления по указанным в согласии адресам.

(дата)

(подпись)

(расшифровка подписи)

**Поставщик:**

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

**Покупатель:**

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.



## **СУБЛИЦЕНЗИОННЫЙ ДОГОВОР**

**Акционерное общество «Петербургская сбытовая компания» (АО «Петербургская сбытовая компания»)**, именуемое в дальнейшем «Сублицензиат», в лице директора по информационным технологиям Белокурова Михаила Ивановича, действующего на основании доверенности № 876/1/2021 от 21.12.2021, с одной стороны и

**Общество с ограниченной ответственностью «Бизнес Коммуникации» (ООО «БизКомм»)**, именуемое в дальнейшем «Лицензиат», в лице Заместителя генерального директора Пестунова Александра Владиславовича, действующего на основании доверенности от 18.08.2021 № 27, с другой стороны, совместно именуемые «Стороны», заключили настоящий Сублицензионный Договор о нижеследующем:

### **1. Основные понятия, применяемые в настоящем Сублицензионном Договоре**

- 1.1. **Программа для ЭВМ («программное обеспечение» или «программа»)** – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.
- 1.2. **Стандартная версия программы для ЭВМ** – версия программы для ЭВМ, действующая у Лицензиата, в момент заключения Сублицензионного Договора.
- 1.3. **Новая версия программы для ЭВМ** – версия программы для ЭВМ, созданная на базе стандартной версии программы в результате произведенных улучшений.
- 1.4. **Индивидуальная версия программы для ЭВМ** – версия программы для ЭВМ, созданная по индивидуальному заказу.
- 1.5. **Демонстрационная версия программы для ЭВМ** – показательное изложение программы для ЭВМ, не поддерживающее всех функций программы.
- 1.6. **Комплект программного обеспечения** – набор овеществленных носителей на объекты исключительных прав, передаваемых от Лицензиата Сублицензиату, который может включать в себя:
  - копию (экземпляр) программного обеспечения на CD-диске или ином носителе;
  - инструкцию по инсталляции на CD-диске или ином носителе,
  - руководство пользователя программного обеспечения на CD-диске или ином носителе.
- 1.7. **Индивидуальная информация Лицензиата** - данные, которые Лицензиат предоставляет Сублицензиату для внесения в программное обеспечение, с целью его адаптации к условиям работы в конкретном субъекте федерации, городе, регионе, области, округе, муниципальном образовании, сельском (поселковом) поселении и др.

### **2. Предмет Сублицензионного Договора**

- 2.1. Лицензиат обязуется предоставить Сублицензиату неисключительные права на использование программного обеспечения на условиях настоящего Сублицензионного Договора и выдать простую (неисключительную) лицензию на бумажном носителе, на основании которой (которых) Сублицензиат вправе пользоваться сам и предоставить право использования программным обеспечением своим структурным подразделениям.
- 2.2. Сублицензиат обязуется уплатить Лицензиату вознаграждение за предоставленное право на использование программного обеспечения в размере и на условиях, установленных настоящим Сублицензионным Договором.
- 2.3. Предоставление прав на использование программного обеспечения сопровождается передачей Сублицензиату Комплекта программного обеспечения и Лицензии (либо лицензий) на использование программного обеспечения.
- 2.6. Перечень передаваемого по Сублицензионному Договору программного обеспечения определен в **Приложении № 1 к Договору поставки № 22-100 от 03.03.2022 г.**
- 2.7. Количество комплектов программного обеспечения с лицензиями, предоставляющими право на использование стандартных определяется в соответствии с **Приложением № 1 к Договору поставки № 22-100 от 03.03.2022 г.**



2.8. Функциональные характеристики стандартной версии программного обеспечения, действующей на момент заключения Сублицензионного Договора и входящей в комплект программного обеспечения определяются Сторонами.

2.9. Объем прав Сублицензиата на использование программного обеспечения установлен настоящим Сублицензионным Договором.

### **3. Права и обязанности Лицензиата**

#### **3.1. Права Лицензиата:**

3.1.1. Лицензиату принадлежат права на использование программного обеспечения, включая использование следующими способами: путем распространения программ для ЭВМ конечным пользователям, находящимся на территории России; путем воспроизведения программ для ЭВМ, ограниченного инсталляцией, копированием и запуском программ для ЭВМ в соответствии с лицензионным соглашением для конечного пользователя, предоставляемое с единственной целью передачи прав использования этим способом конечным пользователем, находящимся на территории России. При этом право на использование программы для ЭВМ, в отношении которого предоставляется простая (неисключительная) лицензия, ограничено пределами, предусмотренными лицензионным соглашением для конечного пользователя. Лицензиат гарантирует, что он обладает всеми правами, необходимыми для заключения и исполнения настоящего Сублицензионного Договора.

3.1.2. Лицензиат вправе требовать выплаты вознаграждения за предоставленное право на использование программного обеспечения.

3.1.3. В случае нарушения прав Лицензиат вправе осуществлять защиту своих прав в порядке и способами, предусмотренными законом, в том числе Лицензиат вправе требовать от нарушителя возмещения причиненного ущерба, подтвержденного документально.

#### **3.2. Обязанности Лицензиата:**

3.2.1. Лицензиат обязан предоставить Сублицензиату программное обеспечение, указанное в п. 2.6. настоящего Сублицензионного Договора для использования, передав Сублицензиату Комплекты программного обеспечения в количестве, установленном в п. 2.7. Сублицензионного Договора в сроки, определенные **Договором поставки № 22-100 от 03.03.2022 г.**

3.2.2. Лицензиат обязан выдать Сублицензиату лицензию (либо лицензии) на использование программного обеспечения, в которой должны быть отражены основные условия Сублицензионного Договора.

3.2.3. Техническая поддержка Сублицензиату по программному обеспечению оказывается Правообладателем, в том числе, но не ограничиваясь нижеизложенным:

оказание по телефону технической помощи в решении возникших проблем и проведение консультаций Сублицензиата по программному обеспечению;

поддержку адреса электронной почты в сети «Интернет» («Internet»), указанного в разделе 16 **Договора поставки № 22-100 от 03.03.2022 г.**, для приема запросов Сублицензиата на оказание технического содействия;

предоставление Новых версий программного обеспечения без взимания каких-либо дополнительных лицензионных платежей.

3.2.4. Обеспечить неразглашение персональной информации о Сублицензиате, его работниках или партнерах, а также иной информации (в т.ч. о модели компьютеров, об установленных на них иных программных продуктах, пользовательских настройках или хранящихся на компьютерах данных), ставшей известной Лицензиату в процессе исполнения или заключения Сублицензионного Договора. Использовать указанную информацию только для того, чтобы исполнить Сублицензионный Договор, не использовать ни в каких других целях, позволяющих третьим лицам идентифицировать Лицензиата.

### **4. Права и обязанности Сублицензиата**

#### **4.1. Сублицензиат вправе:**

4.1.1. Осуществлять эксплуатацию программного обеспечения в соответствии с его назначением, в том числе запись и хранение в памяти ЭВМ.

4.1.2. Изготовить копию программы при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал программы утерян, уничтожен или стал непригоден для использования. При этом копия программы не может быть использована для иных целей, кроме целей указанных в настоящем Сублицензионном Договоре и должна быть возвращена Лицензиату либо уничтожена в случае, если владение экземпляром этой программы перестает быть правомерным.

4.1.3. Сублицензиат не обязан представлять Лицензиату отчеты об использовании программ.

#### **4.2. Сублицензиат обязан:**



- 4.2.1. Не допускать действий, влекущих за собой нарушение прав Лицензиата.
- 4.2.2. Своевременно производить оплату вознаграждения за право пользования программным обеспечением, а также консультационных услуг в соответствии с условиями настоящего Сублицензионного Договора.

## **5. Цена Сублицензионного Договора. Порядок расчетов**

- 5.1. Размер вознаграждения, подлежащего уплате Лицензиату за предоставление неисключительного права на использование программного обеспечения, определяется в соответствии с **Договором поставки № 22-100 от 03.03.2022 г.**, НДС не облагается на основании пункта 2 подпункта 26 ст.149 Налогового кодекса РФ. Программное обеспечение включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.
- 5.2. Сублицензиат производит оплату вознаграждения по Сублицензионному Договору на основании счетов, предъявленных к оплате Лицензиатом в порядке, указанном в **Договоре поставки № 22-100 от 03.03.2022 г.**
- 5.3. Цена настоящего Сублицензионного Договора определяется в валюте Российской Федерации (рубли). Датой осуществления платежа признается дата списания денежных средств с расчетного счета Лицензиата.

## **6. Порядок сдачи и приемки экземпляров программного обеспечения и оказанных услуг**

- 6.1. Программное обеспечение передаётся представителю Сублицензиата лично с подписанием сторонами Акта приема-передачи лицензии (программного обеспечения). Акт приема-передачи составляет Лицензиат и предоставляет Сублицензиату совместно с программным обеспечением.
- 6.2. Передача комплекта (комплектов) программного обеспечения в количестве, указанном в п. 2.7. настоящего Сублицензионного Договора, производится по адресу Склада, указанному в **Договоре поставки № 22-100 от 03.03.2022 г.**
- 6.3. Датой получения комплекта (комплектов) программного обеспечения Сублицензиатом считается дата подписания сторонами Акта приема-передачи лицензии (программного обеспечения).
- 6.4. Проверка наименования, комплектации, иных данных, касающихся предоставляемых прав использования программ, осуществляется Сублицензиатом не позднее 5 (пяти) рабочих дней с момента предоставления указанных прав. Подписание Акта приема-передачи не лишает Сублицензиата права ссылаться на недостатки переданных прав использования программ и предъявлять соответствующие требования к Сублицензиату. В случае выявления каких-либо несоответствий Стороны составляют соответствующий акт.
- 6.5. Проверка наименования, комплектации, иных данных, касающихся предоставляемых прав использования программ, осуществляется Сублицензиатом не позднее 5 (пяти) рабочих дней с момента предоставления указанных прав. Подписание Акта приема-передачи не лишает Сублицензиата права ссылаться на недостатки переданных прав использования программ и предъявлять соответствующие требования к Лицензиату. В случае выявления каких-либо несоответствий Стороны составляют соответствующий акт.

## **7. Ответственность сторон. Действие непреодолимой силы**

- 7.1. Настоящий раздел читается в соответствии с разделом 9 «Ответственность по Договору» и разделом 10 «Форс-мажор» **Договора поставки № 22-100 от 03.03.2022 г.**

## **8. Прочие условия**

- 8.1. Права на использование программного обеспечения, переданные по настоящему Договору, не могут передаваться Сублицензиатом полностью или частично другим лицам.
- 8.2. Ни Сублицензиат, ни пользователи программного обеспечения не вправе без предварительного письменного согласования Лицензиата распространять экземпляры программного обеспечения или его версии любым способом, передавать его третьим лицам, вносить изменения в программное обеспечение, переделывать программное обеспечение.
- 8.3. Все изменения и дополнения к настоящему Сублицензионному Договору считаются действительными, если они оформлены в письменном виде и подписаны обеими Сторонами.
- 8.4. Условия настоящего Сублицензионного Договора конфиденциальны и не подлежат разглашению. Если иное не будет установлено соглашением Сторон, конфиденциальными являются также все получаемые Сторонами друг от друга в процессе исполнения Сублицензионного Договора сведения, за исключением тех, которые без участия Сторон были или будут опубликованы, или распространены в официальных источниках, либо иным образом стали/станут публично известны. При этом ни одна из



Сторон не несет ответственности за действия, связанные с представлением конфиденциальных сведений в суд или иной компетентный государственный орган на основании их официального запроса.

8.5. Разрешение споров по настоящему Сублицензионному договору производится в соответствии с разделом 13 «Разрешение споров» Договора поставки № 22-100 от 03.03.2022 г.

#### 9. Срок предоставления прав и действия Сублицензионного Договора<sup>5</sup>

9.1. Настоящий Сублицензионный Договор вступает в силу с даты его подписания Сторонами и действует по истечении 1 (одного) календарного года с момента активации сервиса технической поддержки.

9.2. Сублицензионный Договор может быть расторгнут в случаях, описанных в разделе 13 «Основания расторжения договора» Договора поставки № 22-100 от 03.03.2022 г.

#### 10. Заключительные положения

10.1. Во всем ином, не предусмотренным настоящим Сублицензионным Договором и Договором поставки № 22-100 от 03.03.2022 г., Стороны руководствуются действующим законодательством РФ.

10.2. Настоящий Сублицензионный Договор составлен в двух подлинных экземплярах, имеющих одинаковую юридическую силу, по одному для каждой стороны.

#### 11. Адреса и реквизиты сторон

Лицензиат:	Сублицензиат:
ООО «БизКомм» ИНН 7714856880 КПП 772401001 ОГРН 1117746926593 Юридический адрес: 115230, г. Москва, проезд Хлебозаводский, д. 7, стр. 9, эт. 3, пом. X, ком. 25, оф. 14 Почтовый адрес: 119334, г. Москва, а/я 85 ОКПО 37215155 ОКТМО 45918000 e-mail: in@biz-komm.ru телефон: +7 (495) 900-10-65 Банковские реквизиты: р/с 40702810747010001406 в ЦЕНТРАЛЬНЫЙ ФИЛИАЛ АБ "РОССИЯ" к/с 30101810145250000220 БИК 044525220	АО «Петербургская сбытовая компания» ИНН 7841322249 КПП 780401001 ОГРН 1057812496818 Юридический адрес: 195009, Санкт-Петербург, ул. Михайлова, дом 11 Почтовый адрес: 195009, Санкт-Петербург, ул. Михайлова, дом 11 ОКПО 77724330 ОКТМО 40330000000 e-mail: office@pesc.ru телефон: +7 (812) 303-69-69 факс: +7 (812) 327-07-03 Банковские реквизиты: р/с 40702810900000028772 в БАНК ГПБ (АО) г. Москва БИК 044525823 к/с 30101810200000000823
Заместитель генерального директора  _____ Пестунов А.В.	Директор по информационным технологиям  _____ Белокуров М.И.

<sup>5</sup> Согласно п.4 ст.1235 ГК РФ указанный срок не может превышать срок действия исключительного права на результат интеллектуальной деятельности или на средство индивидуализации.





**Форма предоставления заказчику информации о стране происхождения товара, в том числе поставляемого при выполнении закупаемых работ, оказании закупаемых услуг**

№ п/п	Код товара по Общероссийскому классификатору продукции по видам экономической деятельности ОК 034-2014 (КПЕС 2008) (ОКПД2)	Номер реестровой записи товара в реестрах, предусмотренных пунктом 2 Постановления № 2013 <sup>6</sup> (при наличии)	Наименование товара	Объем товара, в том числе поставленного при выполнении закупаемых работ, оказаниикупаемых услуг (рублей)	Объём российского товара, в том числе товара, поставленного при выполнении закупаемых работ, оказании закупаемых услуг (рублей)
1.	26.2 - Компьютеры и периферийное оборудование	Отсутствует	Сервер ThinkSystem SR530, форм фактор Rack 1U, установка до 2 процессоров, 12 слотов под оперативную память TruDDR4 2666МГц до 768Гб, установка до 8 жестких дисков 2,5" SAS/SATA, сетевой интерфейс 10GbE 2P, установка до 2 блоков питания с горячей заменой, в составе: ThinkSystem SR530 2.5" Chassis with 8 Bays (AV0S), Operating mode	8 119 454,40	

<sup>6</sup> Поименный реестровой записи товара, включенного в реестр промышленной продукции, произведенной на территории Российской Федерации, или в реестр промышленной продукции, произведенной на территории государства - члена Евразийского экономического союза, за исключением Российской Федерации, предусмотренные постановлением Правительства Российской Федерации от 30 апреля 2020 г. N 616 "Об установлении запрета на допуск промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд, а также промышленных товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок для нужд обороны страны и безопасности государства ИЛИ в единый реестр российской радиоэлектронной продукции, предусмотренный постановлением Правительства Российской Федерации от 10 июля 2019 г. N 878 "О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" и признании утратившими силу некоторых актов постановления Правительства Российской Федерации от 16 сентября 2016 г. N 925 и признании утратившими силу некоторых актов Правительства Российской Федерации.



			<p>selection for: Efficiency  - Favoring Performance Mode (BFYE), Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor (B7N6) 2шт,  ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM (B4H2) 4шт,  ThinkSystem SR530/SR630/SR570 2.5" SATA/SAS 8-Bay Backplane (AUWB),  Select Storage devices - no configured RAID required (5977),  ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E),  ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD (AUM1) 4шт,  ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit (AUWC),  ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit (AUWA),  Lenovo ThinkSystem 1U LP+LP BF Riser Bracket (AUWQ),  ThinkSystem 1Gb 2-port RJ45 LOM (AUKG), T</p>		
2.	26.2 - Компьютеры и периферийное оборудование	Отсутствует	<p>Сервер ThinkSystem SR590, форм-фактор 2U, в составе: ThinkSystem SR590 3.5" Chassis with 8 or 12 Bays (AXEB), Operating mode selection for:</p>	4 547 604,00	



"Efficiency - Favoring Performance Mode" (BFYE), Intel Xeon Gold 6230R 26C 150W 2.1GHz Processor (BAZX) 2шт, ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM (B4H3) 4шт, ThinkSystem 2U 3.5" SATA/SAS 12-Bay Backplane (AUR9), Select Storage devices - no configured RAID required (5977), ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E), ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD (AUU8) 12шт, ThinkSystem M.2 with Mirroring Enablement Kit (AUMV), ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD (B8HS) 2шт, ThinkSystem SR590 x8/x8/x8 PCIe Riser 1 (B261), ThinkSystem 10Gb 2-port SFP+ LOM (AUKJ), ThinkSystem Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter (AUKX), ThinkSystem 750W(230/115V) Platinum Hot-Swap Power Supply (AXE6) 2шт, 2.8m, 13A/100-250V, C13 to C14



			Jumper Cord (6400) 2шт, ThinkSystem XClarity Controller Stand		
3.	26.2 - Компьютеры и периферийное оборудование	Отсутствует	Сервер ThinkSystem SR650, форм фактор Rack 2U, в составе: SR650 3,5 Chassis with 8 or 12 bays (AUVW), Operating mode selection for: "Efficiency - Favoring Performance Mode" (BFYE), INTEL Xeon Gold 6230R 26C 150W 2.1GHz (BAZX) 2шт, ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM (B4H3) 8шт, ThinkSystem 2U 3.5" SATA/SAS 12-Bay Backplane (AUR9), select storage devices no configured RAID required (5977), ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter (B31E), ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD (B8HQ) 6шт, ThinkSystem M.2 with Mirroring Enablement Kit (AUMV), ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD (B8HS) 2шт, ThinkSystem 2U x8/x8/x8 PCIE FH Riser 1 (AUR4), ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet	6 765 542,40	



			Adapter (AUZY), ThinkSystem Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter (AUKX), ThinkSystem 1100W (230V/115V) Platinum Hot-Swap Power Supply (AVWF) 2шт, 2.8m, 13A/100-250V, C13 to C14 Jumper Cord (6400) 2шт, ThinkSystem XClarity Contr		
--	--	--	--	--	--

**Поставщик:**

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

**Покупатель:**

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.



## СОГЛАШЕНИЕ ОБ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

Акционерное общество «Петербургская сбытовая компания» (АО «Петербургская сбытовая компания»), именуемое в дальнейшем «Сторона-1», в лице директора по информационным технологиям Белокурова Михаила Ивановича, действующего на основании доверенности № 876/1/2021 от 21.12.2021, с одной стороны, и

Общество с ограниченной ответственностью «Бизнес Коммуникации» (ООО «БизКомм»), именуемое в дальнейшем «Сторона-2», в лице Заместителя генерального директора Пестунова Александра Владиславовича, действующего на основании доверенности от 18.08.2021 № 27, с другой стороны, совместно именуемые в дальнейшем «Стороны», заключили настоящее соглашение (далее – «Соглашение») о нижеследующем.

Настоящее Соглашение является неотъемлемой частью Договора поставки № 22-100 от 03.03.2022 (далее — Соглашение).

### 1. Термины, определения и сокращения

1.1. Все термины и определения используются в настоящем Соглашении и при взаимодействии Сторон на основании Соглашения в следующем значении:

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Аккредитованный удостоверяющий центр	АУЦ	Юридическое лицо, осуществляющее функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные действующим законодательством
Владелец квалифицированного сертификата ключа проверки электронной подписи	Владелец КЭП	Лицо, которому в установленном действующим законодательством порядке выдан квалифицированный сертификат ключа проверки электронной подписи
Исправленный УПД		Электронный первичный документ об отгрузке товаров (выполнении работ), передаче имущественных прав (документ об оказании услуг), применяемый при оформлении фактов хозяйственной жизни, содержащий данные счета-фактуры оформляемый участниками оборота товаров для исправления ранее составленного документа, содержавшего ошибки и (или) неточности
Квалифицированная электронная подпись	КЭП	Вид усиленной электронной подписи, которая отвечает всем признакам, установленным Федеральным законом № 63-ФЗ «Об электронной подписи», в том числе следующим: – получена в результате криптографического преобразования информации с использованием ключа электронной подписи; – позволяет определить лицо, подписавшее электронный документ; – позволяет обнаружить факт внесения изменений в электронный документ после его подписания; – создается с использованием средств электронной подписи; – ключ проверки электронной подписи указан в сертификате ключа проверки электронной подписи; – для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи»
Квалифицированный сертификат ключа проверки электронной	Сертификат КЭП	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным



подписи		Федеральным законом № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом
Ключ проверки электронной подписи	Открытый ключ	Уникальная последовательность символов, которая создается в паре с закрытым ключом электронной подписи с помощью криптографического алгоритма и используется для шифрования данных и проверки подлинности электронной подписи в электронном документе
Ключ электронной подписи	Закрытый ключ	Уникальная последовательность символов, предназначенная для создания электронной подписи в электронных документах
Компрометация ключа электронной подписи		Утрата доверия к тому факту, что используемые закрытые ключи электронной подписи неизвестны посторонним лицам. Также под компрометацией ключа электронной подписи понимается его утрата, хищение, разглашение, несанкционированное копирование, любые другие виды разглашения закрытого ключа ЭП, а также такие случаи, когда нельзя достоверно установить, что произошло с носителем, содержащим закрытый ключ ЭП
Направляющая Сторона		Сторона-1 или Сторона-2, направляющая электронный документ, подписанный ЭП по телекоммуникационным каналам связи другой Стороне
Неформализованный электронный документ		Электронный документ, исполненный в формате, не установленном законодательством РФ или в формате, самостоятельно разработанном Обществом
Оператор электронного документооборота	Оператор ЭДО	Организация, соответствующая установленным действующим законодательством требованиям к оператору электронного документооборота и предоставляющая услуги по обмену открытой и конфиденциальной информацией по телекоммуникационным каналам связи в рамках обеспечения электронного документооборота между Компанией и третьими лицами с применением электронных подписей
Первичный учетный документ		Для целей настоящего документа: документ, которым оформляется факт хозяйственной операции для целей отражения в бухгалтерском и налоговом учете
Получающая Сторона		Сторона-1 или Сторона-2, получающая от направляющей Стороны электронный документ, подписанный ЭП, по телекоммуникационным каналам связи
Роуминг (межоператорское взаимодействие)		Технология, обеспечивающая возможность обмена электронными документами между разными операторами электронного документооборота
Сертификат ключа проверки электронной подписи	Сертификат ЭП	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи Владельцу сертификата ключа проверки электронной подписи
Уведомление об уточнении документа	УОУ	Электронный файл установленного формата, фиксирующий факт несогласия получающей Стороны с полученным электронным документом
Универсальный корректировочный документ	УКД	Электронный документ, применяемый при подтверждении факта согласования продавцом и покупателем изменения (уведомления продавцом покупателя об изменении) стоимости договора в связи с изменением цены (тарифа) и (или) уточнения количества





		(объема) поставленных (отгруженных) товаров (выполненных работ, оказанных услуг), переданных имущественных прав
Универсальный передаточный документ	УПД	Электронный документ, применяемый для оформления фактов хозяйственной жизни и/или при расчетах по налогу на добавленную стоимость, формат которого утверждается Федеральной налоговой службой, который может применяться в одной из следующих функций: <ul style="list-style-type: none"> <li>– СЧФДОП - Счет-фактура, применяемый при расчетах по налогу на добавленную стоимость, и документ об отгрузке товара, выполнении работ, передаче имущественных прав, документ об оказании услуг;</li> <li>– СЧФ – Счет-фактура, применяемый при расчетах по налогу на добавленную стоимость;</li> <li>– ДОП – Документ об отгрузке товара, выполнении работ, передаче имущественных прав, документ об оказании услуг</li> </ul>
Формализованный электронный документ		Электронный документ, исполненный формате, установленном или рекомендованном законодательством РФ
Электронный документ	ЭД	Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах
Электронный документооборот	ЭДО	Комплекс автоматизированных процессов, обеспечивающих движение электронных документов с момента их создания и/или получения до завершения их обработки, архивирования и/или уничтожения
Электронная подпись	ЭП	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и применяется для определения лица, подписывающего информацию

## 2. Предмет соглашения

2.1. Настоящим Соглашением Стороны устанавливают условия и порядок организации обмена электронными документами по телекоммуникационным каналам связи, подписанными КЭП в качестве аналога собственноручной подписи и печати организации.

2.2. Стороны соглашаются признавать полученные (направленные) в рамках электронного документооборота электронные документы равнозначными аналогичным документам на бумажных носителях.

2.3. Электронные документы, которыми обмениваются Стороны в рамках ЭДО, должны быть подписаны квалифицированной ЭП.

2.4. Электронный документооборот осуществляется Сторонами посредством обмена видами электронных документов, указанных в Приложении 1 к Соглашению.

2.4.1. В случае если нормативно-правовые акты, указанные в Приложении 1 Соглашения, будут отменены либо изменены, Стороны обязуются применять форматы формализованных документов, утвержденные действующими на соответствующую дату нормативно-правовыми актами Российской Федерации.

2.4.2. В случае, если вступят в силу нормативно-правовые акты в отношении утверждения форматов документов, указанных в п. Приложении 1 к Соглашению, такие документы должны формироваться с учетом вступивших в силу нормативно-правовых актов.

2.5. Документы, не перечисленные в Приложении 1 к Соглашению, переданные по электронным каналам связи, не являются согласованными к переходу в ЭДО, даже если они отвечают всем требованиям, предъявляемым к ЭД и подписаны КЭП. В дальнейшем ни одна из Сторон не вправе ссылаться на указанные документы в качестве подтверждения исполнения ими своих обязательств.



### 3. Общие принципы электронного документооборота и применения электронной подписи

3.1. Электронный документооборот Стороны осуществляют в соответствии с нормами законодательства Российской Федерации, условиями настоящего Соглашения и иных соглашений и договоров, заключенных между Сторонами, а также с учетом положений регламентирующих документов Оператора ЭДО.

3.2. При выставлении и получении УПД СЧФ / СЧФ ДОП в электронном виде Стороны руководствуются утвержденными нормативно-правовыми актами Российской Федерации, действующими на соответствующую дату.

3.3. Квалифицированные сертификаты ключей проверки ЭП приобретаются Сторонами в аккредитованных удостоверяющих центрах, ключи ЭП создаются сертифицированными Федеральной службой безопасности Российской Федерации средствами ЭП Сторон или с привлечением аккредитованного удостоверяющего центра, выпустившего квалифицированный сертификат ЭП.

3.4. Документы формируются, передаются и принимаются Сторонами в электронном виде без их последующего обязательного представления на бумажном носителе. Электронный документооборот между Сторонами не отменяет возможности использования иных способов обмена документами между Сторонами.

3.5. Стороны признают, что ответственность за обеспечение конфиденциальности, целостности и доступности информации с момента передачи электронного документа Оператору ЭДО любой из Сторон несет Оператор ЭДО/Операторы ЭДО.

3.6. Стороны признают, что использование средств криптографической защиты информации, достаточно для подтверждения того, что:

- электронный документ исходит от Стороны, его передавшей (подтверждение авторства документа);
- электронный документ не претерпел изменений при информационном взаимодействии Сторон (подтверждение целостности и подлинности документа) при положительном результате проверки ЭП.

3.7. Датой направления электронного документа является дата его поступления Оператору ЭДО направляющей Стороной, указанная в протоколе передачи документа. Электронные документы, направленные в рамках настоящего Соглашения, считаются полученными принимающей Стороной с даты присвоения им соответствующего статуса в системе Оператора ЭДО, подтверждающего их доставку принимающей Стороне, указанной в протоколе передачи документа.

3.8. Дата формирования подписи электронного документа определяется на основании информации, указанной Оператором ЭДО в протоколе передачи документа.

3.9. Датой подписания договора или дополнительного соглашения является дата подписания второй Стороной последнего сформированного к договору или дополнительному соглашению протокола разногласий, зафиксированная Оператором ЭДО в протоколе передачи документа.

3.10. Стороны обязаны незамедлительно информировать друг друга о невозможности обмена электронными документами, подписанными ЭП, в частности в следующих случаях:

- недоступность системы Оператора ЭДО;
- поврежденность или недоступность каналов связи;
- сбой учетной системы Сторон;
- истечение срока действия квалифицированного сертификата ЭП (до момента получения квалифицированного сертификата ЭП с новым сроком действия);
- иные случаи, не позволяющие производить обмен электронными документами.

3.11. В период, когда обмен электронными документами невозможен, Стороны производят обмен документами на бумажных носителях, подписанными уполномоченными представителями Сторон собственноручной подписью.

3.12. Стороны обязаны незамедлительно информировать друг друга о прекращении обстоятельств, обуславливающих невозможность обмена электронными документами, после чего возобновить обмен электронными документами.

3.13. Информирование Сторонами о невозможности обмена электронными документами, а также о прекращении обстоятельств, обуславливающих невозможность обмена электронными документами, осуществляется путем направления уведомления на адреса электронной почты, согласованные Сторонами.

3.14. В случае, если дата составления первичного учетного документа отличается от даты совершения факта хозяйственной жизни, первичный учетный документ должен содержать дату совершения факта хозяйственной жизни.

3.15. При обмене электронными документами Стороны обязуются заполнять следующие данные в соответствующих полях:



– при отправке первого электронного документа адрес электронной почты получателя документа у Принимающей Стороны, номер и дата договора при отправке всех документов, относящихся к конкретному договору, указываются в полях документа и/или сопровождающих документ метаданных в системе оператора ЭДО, исходя из требований пунктов 3.14 и 3.15 настоящего Соглашения.

3.16. При оформлении документов через web-интерфейс Контур.Диадок данные поля заполняются следующим образом:

- для формализованных документов, а также для неформализованных дополнительных соглашений и ценовых листов данные по договору указываются в поле «основание»,
- для иных неформализованных документов данные по договору указываются в свободном поле для комментариев,
- для всех видов документов адрес электронной почты получателя указывается в свободном поле для комментариев.

3.17. При оформлении документов иным способом подход к заполнению данных полей определяется Сторонами дополнительно.

3.18. В случае повторного составления электронного документа или составления электронного документа на отмененную операцию, Стороны применяют аннулирование документов, за исключением случаев корректировки или исправления документов, предусмотренных действующим законодательством. При аннулировании документов, передаваемых через Оператора ЭДО, Стороны используют формат электронного соглашения об аннулировании, который поддерживается операторами ЭДО.

3.19. Процесс аннулирования электронных документов через Оператора ЭДО предполагает следующий порядок действий сторон:

- принимающая/направляющая Сторона направляет второй Стороне предложение об аннулировании документа с указанием причины аннулирования документа;
- если вторая Сторона согласна аннулировать документ и признает документ недействительным, то под соглашением необходима подпись второй Стороны. Когда вторая Сторона подпишет соглашение, аннулируемый документ потеряет юридическую силу.
- если вторая Сторона не согласна с предложением об аннулировании, то она имеет право отказать в подписи соглашения. В этом случае электронный документ сохраняет свою юридическую силу.

3.20. В случае, если у Сторон нет возможности подписать соглашение об аннулировании в электронном виде через Оператора ЭДО, Стороны могут оформить данное соглашение на бумажном носителе в свободной форме, с указанием реквизитов аннулированного документа, причины его аннулирования.

3.21. В случае, когда электронный документ еще не подписан получающей Стороной, направляющая Сторона может аннулировать электронный документ в одностороннем порядке.

3.22. Подтверждение аннулирования/отказ от аннулирования должно осуществляться в срок не более 3 рабочих дней с момента получения второй Стороной предложения на аннулирование.

4. Условия признания электронных документов равнозначными документам на бумажном носителе

4.1. Подписанный КЭП электронный документ признается равнозначным аналогичному подписанному собственноручно документу на бумажном носителе и порождает для Сторон юридические последствия в виде установления, изменения и прекращения взаимных прав и обязанностей при одновременном соблюдении следующих условий:

- квалифицированный сертификат ключа проверки ЭП создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на момент выдачи указанного сертификата;
- квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;
- имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания.

4.2. При соблюдении условий, приведенных в п. 4.1 настоящего Соглашения, электронный документ должен приниматься Сторонами к учету и может использоваться в качестве доказательства в судебных разбирательствах, представляться в государственные органы по запросам последних.



4.3. Подписание одного электронного документа двумя Сторонами осуществляется путем последовательного подписания данного электронного документа каждой из Сторон.

4.4. Не допускается отправка документов с одинаковыми номерами и датой. В случае получения одной из Сторон настоящего Соглашения электронного документа с номером и датой соответствующими номеру и дате одного из документов, полученных ранее, такой документ признается недействительным и не имеющим юридической силы. В целях однозначного понимания данного пункта Стороны не признают юридическую силу дубликатов первого электронного документа и принимают к учету только первую версию подписанного Сторонами документа.

## 5. Взаимодействие с операторами электронного документооборота

5.1. Оператором электронного документооборота [Сторон] является АО «Производственная фирма «СКБ Контур» программа для ЭВМ «Диадок».

5.2. До начала осуществления обмена электронными документами, каждая из Сторон обязуется в установленном порядке обеспечить подключение (обеспечить наличие подключения) к системе электронного документооборота Оператора, в том числе заключить соответствующие договоры, оформить и представить Оператору заявление об участии в электронном документообороте, получить у Оператора идентификаторы участника обмена, реквизиты доступа и другие необходимые данные, уведомить об этом другую Сторону (с указанием идентификатора участника обмена).

5.3. По результатам тестового обмена, проверки работоспособности и/или совместимости своих технических средств, Стороны подтверждают, факт проведения успешного тестового обмена различными электронными документами, подтверждающего устойчивую работоспособность и/или совместимость технических средств Сторон, в том числе возможность передачи данных, возможность передачи применяемых форматов.

5.4. С даты подписания настоящего Соглашения, электронные документы, которые направляющая Сторона отправляет в адрес получающей Стороны, признаются равнозначными аналогичным подписанным собственноручной подписью документами на бумажном носителе и порождают для Сторон юридические последствия в виде установления, изменения и прекращения взаимных прав и обязанностей.

5.5. Сторона-2 может использовать услуги Оператора, отличного от указанного в п. 5.1. В этом случае обмен электронными документами между Сторонами осуществляется с использованием роуминга – технологии обеспечивающей возможность обмена электронными документами между разными Операторами.

5.6. В случае, если Сторона-2 пользуется услугами Оператора, отличного от указанного в п.5.1, то такой Оператор должен соответствовать следующим критериям:

- между Оператором Стороны-1, указанным в п. 5.1 настоящего Соглашения, и Оператором Стороны-2 обеспечено роуминговое взаимодействие;
- оператором Стороны-1, указанным в п. 5.1 настоящего Соглашения, и Оператором Стороны-2 подтверждена техническая возможность для приема и передачи всех документов, перечень и форматы которых определены в п. 2.4. настоящего Соглашения.

5.7. Сторона-2 обязуется не позднее 15 (пятнадцати) календарных дней после подписания настоящего Соглашения и в дальнейшем – по мере необходимости, самостоятельно получать в аккредитованном удостоверяющем центре квалифицированные сертификаты ключа проверки ЭП, и обеспечить наличие действующих сертификатов ЭП в течение всего срока действия данного Соглашения.

5.8. В случае прекращения роумингового взаимодействия между Операторами Сторон, равно как и в случае невозможности обмена электронными документами вследствие прекращения таких отношений, Стороны осуществляют обмен документами на бумажном носителе с подписанием их собственноручной подписью и печатью, при ее необходимости.

5.9. В случае, если Сторона намеревается сменить Оператора, услугами которого она пользуется в рамках настоящего Соглашения, такая Сторона обязана не позднее чем за 15 календарных дней до начала обмена электронными документами посредством нового Оператора предоставить другой Стороне документы и сведения, предусмотренные настоящим Соглашением, а также осуществить тестовый обмен.

## 6. Права и обязанности сторон

6.1. Стороны обязуются:

6.1.1. Обеспечить укомплектованность необходимыми программно-техническими средствами для организации работы с электронными документами, включая создание, изменение и обработку, а также обеспечить взаимодействие с системой Оператора ЭДО.

6.1.2. Назначить лиц, ответственных за работу с программно-техническими средствами в соответствии с п. 6.1.1, а также организовать внутренний режим функционирования





ответственных лиц таким образом, чтобы исключить возможность взаимодействия с системой Оператора ЭДО лицами, не имеющими допуска к работе с ней, а также исключить возможность использования ключей ЭП и средств ЭП не уполномоченными на это лицами.

6.1.3. Своевременно производить плановый выпуск ключей ЭП и соответствующих квалифицированных сертификатов ключей проверки ЭП.

6.1.4. Принимать на себя все риски, связанные с работоспособностью своего оборудования и каналов связи.

6.1.5. Не предпринимать действий, способных нанести ущерб другой Стороне вследствие использования ЭДО.

6.1.6. Обмениваться электронными документами, не содержащими компьютерных вирусов и (или) иных вредоносных программ.

6.2. Стороны вправе:

6.2.1. В случае возникновения обстоятельств непреодолимой силы, повлекших нарушение установленного настоящим Соглашением порядка выставления документов в электронном виде, Стороны вправе использовать бумажный документооборот, при этом исполнение обязательств и оплата производится в порядке и сроки, установленные соответствующим договором, в рамках исполнения которого происходит обмен электронными документами.

6.2.2. Ограничивать и приостанавливать использование ЭДО в случаях ненадлежащего исполнения другой Стороной Соглашения с уведомлением не позднее дня приостановления и по требованию компетентных государственных органов – в случаях и в порядке, предусмотренных законодательством Российской Федерации.

6.2.3. Остановить работу Системы ЭДО по техническим причинам до восстановления ее работоспособности.

## 7. Ответственность сторон и риски

7.1. Стороны несут ответственность за содержание любого электронного документа, подписанного КЭП при условии подтверждения подлинности КЭП в соответствии с разделом 4.

7.2. Стороны несут ответственность за конфиденциальность и порядок использования ключей ЭП.

7.3. Сторона, допустившая компрометацию ключа ЭП, несет ответственность за электронные документы, подписанные с использованием скомпрометированного ключа ЭП, до момента официального уведомления об аннулировании (отзыве) соответствующего квалифицированного сертификата ЭП и конкретных документов, подписанных указанным ключом ЭП. Уполномоченное лицо каждой из Сторон, наделенное правами использования ЭП, несет полную ответственность за любые действия, совершаемые с использованием ЭП, включая действия, совершаемые другими лицами, если ключ ЭП стал доступен другим лицам по вине уполномоченного лица каждой из Сторон.

7.4. Сторона, несвоевременно сообщившая о случаях утраты или компрометации ключа ЭП, несет связанные с этим риски.

7.5. Стороны могут быть освобождены от ответственности за неисполнение своих обязательств по Соглашению при наступлении обстоятельств непреодолимой силы, под которыми подразумеваются внешние, чрезвычайные и непредотвратимые при данных обстоятельствах события, которые не существовали во время подписания Соглашения и возникли помимо воли Сторон.

7.6. Сторона, подвергшаяся действию обстоятельств непреодолимой силы, должна в течение 5 (пяти) календарных дней уведомить другую Сторону о возникновении и возможной продолжительности действия обстоятельств непреодолимой силы. Сторона, своевременно не сообщившая о наступлении вышеупомянутых обстоятельств, лишается права ссылаться на них.

7.7. Факт возникновения обстоятельств непреодолимой силы должен быть документально подтвержден компетентным органом.

7.8. В случае невозможности полного или частичного исполнения обязательств вследствие действия обстоятельств непреодолимой силы, фактическая или возможная продолжительность которых составит один месяц или более, Сторона, исполнение обязательств которой не затронуто действием непреодолимой силы, будет иметь право расторгнуть Соглашение полностью или частично без обязательств по возмещению убытков, связанных с его расторжением. Стороны несут ответственность по настоящему Соглашению в соответствии с действующим законодательством Российской Федерации.

## 8. Действие соглашения и его прекращение

8.1. Настоящее Соглашение вступает в силу с даты его подписания Сторонами и действует до полного прекращения обязательств по Договору № 22-100 от 03.03.2022.



8.2. Настоящее Соглашение составлено и подписано в 2 (двух) подлинных идентичных экземплярах собственноручно или с использованием квалифицированной электронной подписи, имеющих одинаковую юридическую силу, – по одному для каждой из Сторон.

8.3. Любая из Сторон имеет право в одностороннем внесудебном порядке отказаться от исполнения настоящего Соглашения, письменно уведомив об этом другую Сторону не менее чем за 1 (один) календарный месяц до даты расторжения Соглашения.

**Сторона-2:**

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.

**Сторона-1:**

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.





Перечень документов, включаемых в состав ЭДО

Формализованные документы			
1	документ об отгрузке товаров (выполнении работ), передаче имущественных прав (документ об оказании услуг), в т. ч. исправленный, в электронной форме, в формате XML	Приказ Федеральной налоговой службы РФ от 19 декабря 2018 г. N ММВ-7-15/820@	КЭП
2	счет-фактура, в т. ч. исправленный, в электронной форме, в формате XML	Приказ Федеральной налоговой службы РФ от 19 декабря 2018 г. N ММВ-7-15/820@;	КЭП
3	документ об отгрузке товаров (выполнении работ), передаче имущественных прав (документ об оказании услуг), включающий в себя счет-фактуру, в т. ч. исправленный, в электронной форме, в формате XML	Приказ Федеральной налоговой службы РФ от 19 декабря 2018 г. N ММВ-7-15/820@	КЭП
4	документ об изменении стоимости отгруженных товаров (выполненных работ, оказанных услуг), переданных имущественных прав, в электронной форме	Приказ Федеральной налоговой службы РФ от 13 апреля 2016 г. N ММВ-7-15/189@;	КЭП
5	корректировочный счет-фактура, в т. ч. исправленный, в электронной форме	Приказ Федеральной налоговой службы РФ от 13 апреля 2016 г. N ММВ-7-15/189@	КЭП
6	документ об изменении стоимости отгруженных товаров (выполненных работ, оказанных услуг), переданных имущественных прав, включающий в себя корректировочный счет-фактуру, в электронной форме	Приказ Федеральной налоговой службы РФ от 13 апреля 2016 г. N ММВ-7-15/189@	КЭП
7	Корректировочный счет-фактура и/или документ, подтверждающего согласие (факт уведомления) покупателя на изменение стоимости отгруженных товаров	Приказ ФНС России от 12.10.2020 N ЕД-7-26/736	КЭП
8	документ по приемке товарно-материальных ценностей и выявленных расхождений, в электронной форме	Приказ Федеральной налоговой службы РФ от 27 августа 2019 г. N ММВ-7-15/423@	КЭП
9	универсальный корректировочный документ (УКД) в формате XML	Приказ ФНС России от 13.04.2016 № ММВ-7-15/189@	КЭП
10	Акт приемки – сдачи работ (услуг), в электронной форме, в формате XML	Приказ ФНС России от 30.11.2015г. № ММВ-7-10/552@;	КЭП
11	товарная накладная ТОРГ 12 в формате XML	Приказ ФНС России от 30.11.2015г. № ММВ-7-10/551@	КЭП

Неформализованные документы	
Вид документа	Применяемый вид ЭП
счета на оплату	КЭП
акты-сверки	КЭП



договоры и дополнительные соглашения, за исключением трудовых договоров, договоров, требующих нотариального удостоверения и/или государственной регистрации, биржевых сделок, сделок на ОРЭМ и иные документы договорного характера, являющиеся неотъемлемой частью хозяйственного Договора, в отношении которого заключено настоящее Соглашение об ЭДО	КЭП
документы, сопровождающие формализованные электронные документы, в том числе приложения к ним	КЭП
иные документы, подтверждающие исполнение хозяйственного Договора, в отношении которого заключено настоящее Соглашение об ЭДО.	КЭП

Обмен неформализованными документами осуществляется в следующих форматах:

- Microsoft Word 97-2010 (.doc);
- Microsoft Excel 97-2010 (.xls);
- Office Open XML (.docx,.xlsx);
- Joint Photographic Experts Group (.jpeg,.jfif,.jpg);
- Rich Text Format (.rtf);
- Portable Document Format (.pdf);
- Текстовый файл (.txt).

Обмен неформализованными документами в форматах, не указанных выше, подлежит дополнительному согласованию Сторонами.

**Сторона-2:**

Заместитель генерального директора

\_\_\_\_\_ Пестунов А.В.



**Сторона-1:**

Директор по информационным технологиям

\_\_\_\_\_ Белокуров М.И.

Идентификатор документа c3fead3f-5eb4-4148-9fe1-0ec50f92cd6b

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

Подписи отправителя:	Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
 Подпись отправителя:	АО "ПЕТЕРБУРГСКАЯ СБЫТОВАЯ КОМПАНИЯ" Белокуров Михаил Иванович, Директор по информационным технологиям	037E5EA60005AE65AD4ABF45DC1296BCB 9 с 21.12.2021 13:00 по 21.12.2022 09:46 GMT+03:00	02.03.2022 18:25 GMT+03:00 Подпись соответствует файлу документа
Подписи получателя:	Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
 Подпись получателя:	ООО "БИЗКОММ" Пестунов Александр Владиславович, Заместитель генерального директора	030DBE0001E8AD24964E508DCD865E8BA 6 с 22.11.2021 18:29 по 22.11.2022 18:20 GMT+03:00	03.03.2022 15:29 GMT+03:00 Подпись соответствует файлу документа

