

ДОГОВОР №

г. Минск

«__»_____ 2025 г.

_____, именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, с одной стороны и открытое акционерное общество «Белорусский межбанковский расчетный центр», именуемое в дальнейшем «Заказчик», в лице _____, действующего на основании _____, с другой стороны, далее именуемые «Стороны», заключили настоящий Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Исполнитель обязуется передать Заказчику межсетевой экран для защиты веб-приложений (WAF) (далее – ПК), что включает в себя дистрибутив ПК, неисключительные имущественные права (лицензии) на программный комплекс сетевого экрана для защиты веб-приложений согласно Спецификации, Перечню технических требований, Техническим требованиям к программному комплексу (Приложение 1 к Договору), ввести программный комплекс в эксплуатацию в соответствии с Требованиями по вводу программного комплекса в эксплуатацию (Приложение 2 к Договору), оказать техническую поддержку в соответствии с Параметрами технической поддержки программного комплекса (Приложение 3 к Договору), а Заказчик обязуется принять и выплатить вознаграждение за право использования ПК, **ввод его в эксплуатацию и техническую поддержку**, в соответствии с условиями настоящего Договора.

1.2. ПК включает в себя:

Дистрибутив ПК;

неисключительные права на основной узел системы управления;

неисключительные права на активные узлы анализа (до 1 000 запросов в секунду).

1.3. Техническая поддержка ПК включает в себя:

услуги по обновлению ПК (по мере тиражирования производителем);

консультационную поддержку (по телефону и/или по электронной почте, и/или через портал технической поддержки) (24×7).

1.4. Исполнитель гарантирует, что он действует в пределах прав и полномочий, предоставленных ему правообладателем ПК, и на момент предоставления (передачи) Заказчику права на использование ПК они не заложены, не арестованы, не являются предметом исков третьих лиц и являются лицензионным продуктом.

2. СРОКИ И УСЛОВИЯ ПЕРЕДАЧИ ПРАВ НА ПРОГРАММНЫЙ КОМПЛЕКС. ВВОД В ЭКСПЛУАТАЦИЮ

2.1. Передача права на ПК происходит посредством передачи ключевых файлов и (или) буквенно-цифровых кодов, предназначенных для активации (приведения в работоспособное полнофункциональное состояние) ПК и осуществляется по электронным каналам связи одновременно с передачей прав на ПК. Дистрибутив ПК *загружаются с официального сайта производителя* (_____). Передача прав на ПК считается совершенной с момента подписания обеими Сторонами акта приема-передачи прав на ПК. Срок действия прав – бессрочно.

2.2. Передача прав на ПК Заказчику осуществляется в течение 10 (десяти) рабочих дней с даты подписания обеими Сторонами настоящего Договора.

2.3. Датой передачи прав на ПК считается дата подписания обеими Сторонами акта приема-передачи прав на ПК. Копия подписанного акта приема-передачи прав на ПК, переданная по факсу или электронной почте, имеет юридическую силу до момента замены на оригинал. В этом случае оригинал документа должен быть передан в течение 5 (пяти) рабочих дней. Заказчик в течение 5 (пяти) рабочих дней с момента получения акта приема-передачи прав на ПК обязан подписать его и вернуть Исполнителю или в тот же срок в письменном виде предоставить Исполнителю мотивированный отказ от приемки прав на ПК, в противном случае права считаются принятыми надлежащим образом. Мотивированный отказ представляется в письменном виде с обоснованием причин.

2.4. Совместно с актом приема-передачи прав на ПК Исполнитель передает Заказчику заверенную в установленном порядке копию действующего сертификата соответствия требованиям Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность.» (ТР 2013/027/ВУ), выданного Оперативно-аналитическим центром при Президенте Республики Беларусь.

2.5. Срок ввода ПК в эксплуатацию – в течение 60 (шестидесяти) рабочих дней с даты передачи неисключительных прав на ПК. Ввод ПК в эксплуатацию подтверждается актом ввода в эксплуатацию с передачей прав на техническую поддержку ПК (далее – Акт ввода в эксплуатацию), подписанным обеими Сторонами. Требования по вводу ПК в эксплуатацию определены в Приложении 2 к настоящему Договору.

Ввод ПК в эксплуатацию осуществляется по адресу: г. Минск, ул. Кальварийская, 7.

2.6. В ходе ввода ПК в эксплуатацию Исполнитель обязан провести обучение работников (пользователей и персонала сопровождения (администрирования)) Заказчика правилам эксплуатации ПК. Обучение проводится поэтапно, по мере необходимости и готовности ПК. Предварительный график, программа и условия обучения работников предоставляются Исполнителем и согласовываются с Заказчиком на этапе подготовки ПК к внедрению.

Обучение работников (пользователей по работе с инструментарием системы (в разрезе их функций)) проводится на площадях Заказчика. Количество обучаемых – ____ человек (*не менее 5 человек*). Продолжительность обучения – ____ часов (*не менее 20 часов*). Обучение работников производится в ходе осуществления работ по вводу ПК в эксплуатацию и подтверждается подписанием Акта ввода в эксплуатацию. Работникам, прошедшим обучение, должен быть выдан документ, подтверждающий прохождение обучения.

3. СРОКИ, ПОРЯДОК И УСЛОВИЯ ОКАЗАНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

3.1. Срок предоставления технической поддержки (гарантийных обязательств): 13 (тринадцать) месяцев с даты ввода ПК в эксплуатацию.

В случае досрочного прекращения технической поддержки (гарантийных обязательств) Исполнитель обязан вернуть Заказчику сумму в размере десяти базовых величин за каждый месяц в котором не будет оказана техническая поддержка (гарантийные обязательства).

3.2. Исполнитель ежемесячно в течение первых 5 (пяти) рабочих дней месяца, следующего за отчетным, представляет Заказчику технический акт сдачи-приемки оказанных услуг, подтверждающий соответствие заявленным параметрам и удовлетворяющий уровню технической поддержки, указанным в Приложении 3 к Договору. Заказчик в течение 5 (пяти) рабочих дней с момента получения технического акта сдачи-приемки оказанных услуг подписывает его или направляет Исполнителю мотивированный отказ от его подписания.

3.3. Исполнитель обеспечивает техническую поддержку в порядке и на условиях, определенных в Приложении 3 к Договору.

3.4. Исполнитель обязуется принимать и регистрировать:
устные обращения (заявки) Заказчика о наличии проблемы по телефонам: _____;
письменные обращения (заявки) Заказчика по электронному адресу: _____, и/или
через портал технической поддержки _____.

3.5. Источник получения обновлений: <ftp://XX.XX.XX.XXX> (*или иной ресурс*). Исполнитель гарантирует, что предоставляемые обновления ПК соответствуют обновлениям от производителя _____.

3.6. В случае изменения канала обмена информацией или источника получения обновлений, Стороны обязуются передать в письменной форме новый список каналов обмена информации или источник получения обновлений в течение 2 (двух) рабочих дней до момента изменения. Заключение дополнительного соглашения к Договору в данном случае не требуется.

4. СТОИМОСТЬ ДОГОВОРА, ПОРЯДОК РАСЧЕТОВ

4.1. Общая стоимость настоящего Договора составляет _____ (_____) белорусских рублей ____ копеек, в том числе НДС по ставке ____% – _____ (_____) белорусских рублей ____ копеек, в том числе:

стоимость ПК составляет _____ (_____) белорусских рублей ____ копеек, в том числе НДС по ставке ____% – _____ (_____) белорусских рублей ____ копеек;

стоимость ввода ПК в эксплуатацию и предоставление технической поддержки ПК (гарантийных обязательств) составляет _____ (_____) белорусских рублей ____ копеек, в том числе НДС по ставке ____% – _____ (_____) белорусских рублей ____ копеек.

Исполнитель представляет Расчет (калькуляцию) стоимости настоящего Договора.

4.2. Заказчик производит оплату по настоящему Договору в следующем порядке:
за ПК в течении 10 банковских дней с даты передачи неисключительных прав на ПК на основании акта приема-передачи прав на ПК;

за оказание услуг по вводу ПК в эксплуатацию и предоставления технической поддержки ПК (гарантийных обязательств) на основании подписанного сторонами Акта ввода в эксплуатацию в соответствии с графиком платежей (*составляется при заключении договора*).

4.3. Источник финансирования – собственные средства Заказчика.

4.4. Общая стоимость настоящего Договора является окончательной и не подлежит изменению на весь срок действия Договора.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Исполнитель имеет право направить Заказчику письменный запрос о предоставлении материалов и/или информации, необходимой для исполнения Договора.

5.2. Исполнитель обязан:

5.2.1. исполнить настоящий Договор в полном объеме, в соответствии с его условиями и в установленные сроки;

5.2.2. уведомлять Заказчика о возникновении обстоятельств, которые препятствуют и/или могут привести к возникновению препятствий надлежащего исполнения настоящего Договора, не позднее чем через 1 (один) рабочий день после возникновения таких обстоятельств;

5.2.3. не использовать охраняемые результаты интеллектуальной деятельности, исключительные права на которые принадлежат третьим лицам и у Исполнителя отсутствуют права на использование таких результатов. Исполнитель гарантирует Заказчику, что исполнение Договора не будет нарушать прав других лиц;

5.2.4. по требованию Заказчика своими силами и за свой счет в срок, установленный Заказчиком, устранять недостатки, возникшие по вине Исполнителя;

5.2.5. предоставлять требуемую Заказчику информацию (относящуюся к настоящему Договору) в объеме, форме и в сроки, указанные в обращении;

5.2.6. представить по запросу Заказчика документы, подтверждающие прохождение работниками Исполнителя авторизованных (авторских) курсов. В случае наличия документов на иностранном языке, предоставить их перевод на один из государственных языков Республики Беларусь.

5.3. Заказчик имеет право:

5.3.1. получать информацию о ходе исполнения Договора;

5.3.2. запросить у Исполнителя документы, подтверждающие прохождение авторизованных (авторских) курсов.

5.4. Заказчик обязан оказывать Исполнителю необходимое содействие в исполнении Договора.

5.5. Стороны обязуются осуществлять обработку персональных данных, ставших им известными в процессе исполнения настоящего Договора, добросовестно и в целях, соответствующих выполнению обязательств по настоящему Договору, соблюдать конфиденциальность персональных данных, обеспечивать безопасность персональных данных при их обработке и соблюдать требования к защите обрабатываемых персональных данных в соответствии с законодательством Республики Беларусь.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Стороны несут имущественную ответственность в соответствии с законодательством Республики Беларусь и условиями настоящего Договора.

6.2. Исполнитель гарантирует, что предоставление обновлений программного комплекса в рамках настоящего Договора не нарушает авторские и иные права третьих лиц.

6.3. За невозможность предоставления технической поддержки ПК (гарантийных обязательств), Исполнитель уплачивает Заказчику штраф в размере десяти базовых величин за каждый месяц в котором не будет оказана техническая поддержка (гарантийные обязательства).

6.4. За нарушение Исполнителем порядка и условий оказания технической поддержки ПК, определенных в Приложении 3 к настоящему Договору, Исполнитель уплачивает Заказчику штраф в размере 5 (пяти) базовых величин за каждый случай нарушения. Размер базовой величины определяется на день уплаты штрафа.

6.5. За нарушение срока передачи прав на ПК (п. 2.2 Договора), Исполнитель уплачивает Заказчику пеню в размере 0,15 % от стоимости договора за каждый календарный день просрочки.

6.6. За нарушение срока ввода программного обеспечения в эксплуатацию (п. 2.5 Договора), Исполнитель уплачивает Заказчику пеню в размере 0,15 % от стоимости договора за каждый календарный день просрочки.

6.7. За нарушение Исполнителем обязательств, предусмотренных п. 2.6 Договора, Исполнитель уплачивает Заказчику штраф в размере 5 (пяти) базовых величин за каждый случай нарушения. Размер базовой величины определяется на день уплаты штрафа.

6.8. При несвоевременной оплате, Исполнитель имеет право требовать от Заказчика уплаты Исполнителю пени в размере 0,15 % от суммы несвоевременного платежа за каждый календарный день просрочки.

6.9. Уплата пени и штрафа не освобождает виновную Сторону от исполнения своих обязательств по настоящему Договору.

6.10. В случаях, не предусмотренных настоящим Договором, Стороны несут ответственность за неисполнение либо ненадлежащее исполнение принятых на себя обязательств по настоящему Договору в соответствии с законодательством Республики Беларусь.

7. КОНФИДЕНЦИАЛЬНОСТЬ

7.1. Вся информация, полученная и предоставленная Сторонами в рамках настоящего Договора, является информацией, предоставление и/или распространение которой ограничено, и не подлежит разглашению третьим лицам без письменного согласия другой Стороны, за исключением случаев, предусмотренных законодательством Республики Беларусь.

7.2. Исполнитель обязуется незамедлительно возвратить Заказчику по первому письменному требованию оригиналы и все копии предоставленных документов.

7.3. Стороны будут руководствоваться соглашением о взаимоотношениях в вопросах конфиденциальности, авторских прав и прав промышленной собственности, безопасности от _____ № _____, заключенным между Сторонами, и примут все необходимые и разумные меры, чтобы предотвратить разглашение полученной в ходе исполнения настоящего Договора конфиденциальной информации третьим лицам.

8. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

8.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Договору, если неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после заключения Договора в результате событий чрезвычайного характера, которые Стороны не могли ни предвидеть, ни предотвратить разумными мерами.

8.2. К обстоятельствам непреодолимой силы относятся события, на которые Стороны не могут оказать влияние и за возникновение которых не несут ответственности (например, землетрясения, наводнения, пожары и др.). К обстоятельствам, освобождающим Стороны от ответственности, относятся также объявленные или фактические военные действия, гражданские беспорядки, забастовки (за исключением забастовок персонала Сторон).

8.3. Стороны исполняют свои обязательства независимо от введения санкций, иных схожих по правовой природе ограничительных мер, которые могут прямо или косвенно влиять на возможность исполнения Сторонами настоящего Договора. Введенные санкции не рассматриваются Сторонами как обстоятельства непреодолимой силы, и Стороны обязаны исполнять свои обязательства независимо от их введения.

8.4. Сторона, ссылающаяся на такие обстоятельства, обязана в течение 10 (десяти) дней в письменной форме информировать другую Сторону о наступлении подобных обстоятельств. Обстоятельства непреодолимой силы должны быть подтверждены документами компетентных государственных органов.

8.5. Сторона, которая не может из-за обстоятельств непреодолимой силы выполнить обязательства по настоящему Договору, должна приложить все усилия к тому, чтобы как можно скорее осуществить это выполнение.

8.6. После прекращения действия указанных обстоятельств Сторона обязана в течение 10 (десяти) дней сообщить об этом другой Стороне в письменной форме, указав при этом срок, к которому предполагается выполнить обязательства.

8.7. В случае не направления или несвоевременного направления уведомлений, предусмотренных пп. 8.4 и 8.6 настоящего Договора, Сторона не вправе ссылаться на обстоятельства непреодолимой силы, и обязуется возместить другой Стороне причиненные этим убытки.

8.8. В случае возникновения обстоятельств непреодолимой силы срок выполнения обязательств по настоящему Договору отодвигается соразмерно времени, в течение которого действуют такие обстоятельства и их последствия.

8.9. Если обстоятельства непреодолимой силы продолжают действовать более 2 (двух) месяцев, то каждая Сторона имеет право расторгнуть настоящий Договор и обязуется возвратить все полученное ей по Договору, либо произвести расчеты за фактически выполненные обязательства.

9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

9.1. Стороны должны приложить все усилия, чтобы путем прямых переговоров прийти к

обоюдному удовлетворению Сторон всех противоречий или спорных вопросов, возникающих между ними в рамках настоящего Договора.

9.2. Если Стороны не смогут решить спорный вопрос по исполнению настоящего Договора путем переговоров, любая Сторона может потребовать разрешения этого вопроса в экономическом суде г. Минска в установленном законодательством порядке. Претензионный порядок урегулирования споров Стороны признают обязательным. Сторона, получившая претензию, в течение 10 (десяти) рабочих дней письменно извещает заявителя претензии о результатах ее рассмотрения.

9.3. Во всем остальном, что не предусмотрено условиями настоящего Договора, Стороны руководствуются законодательством Республики Беларусь.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Договор вступает в силу и становится обязательным к исполнению для каждой из Сторон с даты его подписания последней из Сторон и действует до полного исполнения Сторонами своих обязательств.

10.2. В случае неисполнения одной из Сторон своих обязательств другая Сторона вправе направить виновной Стороне письменное уведомление, определяющее такое неисполнение, и требование его устранения в течение определенного периода. Если неисполнение не будет устранено за указанный период, потерпевшая Сторона может в любое время в одностороннем порядке отказаться от исполнения Договора (полностью или частично), направив виновной Стороне письменное уведомление, содержащее дату расторжения Договора.

11. АНТИКОРРУПЦИОННАЯ ОГОВОРКА

11.1. Стороны подтверждают, что им известны требования законодательных и иных нормативных правовых актов Республики Беларусь о противодействии коррупции (далее — антикоррупционные требования). Стороны обязуются обеспечить соблюдение антикоррупционных требований и несомнение коррупционных действий при исполнении настоящего Договора своими работниками, представителями, аффилированными лицами, а также субподрядчиками и иными контрагентами, привлекаемыми ими для исполнения настоящего Договора.

11.2. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений настоящего пункта, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящего пункта.

11.3. В случае нарушения одной Стороной обязательств воздерживаться от коррупционных действий и (или) неполучения другой Стороной в десятидневный срок подтверждения, что нарушения не произошло или не произойдет с приложением документов, подтверждающих данный факт, другая Сторона вправе отказаться от настоящего Договора в одностороннем порядке, направив соответствующее письменное уведомление первой Стороне.

11.4. Сторона, нарушившая антикоррупционные требования и (или) не обеспечившая несомнение коррупционных действий при исполнении настоящего Договора своими работниками, представителями, аффилированными лицами, а также субподрядчиками и иными контрагентами, привлекаемыми ими для исполнения настоящего Договора, обязана возместить другой Стороне возникшие у нее в результате этого убытки. Порядок возмещения убытков определяется действующим законодательством Республики Беларусь.

12. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

12.1. Настоящий Договор составлен на русском языке, в двух экземплярах, по одному для каждой из Сторон, имеющих равную юридическую силу.

12.2. Все изменения или дополнения к настоящему Договору действительны в том случае, если они оформлены в виде дополнительных соглашений к настоящему Договору, подписанных уполномоченными представителями Сторон, за исключением изменений местонахождения Сторон и их банковских реквизитов, о чем Стороны письменно информируют друг друга в течение 3 (трех) рабочих дней с момента изменений.

12.3. Ни одна из Сторон не вправе передавать свои права и обязательства по настоящему Договору третьей стороне без письменного согласия на это другой Стороны.

12.4. К Договору прилагается и является его неотъемлемой частью:

Приложение 1. Спецификация, Перечень требований, Требования к программному комплексу.

Приложение 2. Требования по вводу программного комплекса в эксплуатацию.

Приложение 3. Параметры технической поддержки программного комплекса.

Приложение 4. Расчет (калькуляция) стоимости Договора *(составляется по форме Исполнителя)*.

13. Местонахождение, банковские реквизиты и подписи сторон

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:

ОАО «БМРЦ»

ул. Кальварийская, 7, 220048, г. Минск,
Республика Беларусь, тел. +375 17 259 14 85,
факс +375 17 375 34 03

сайт: www.bisc.by;

e-mail: agreement@bisc.by; СМДО: Org10841

ответственное подразделение – Управление
защиты информации в АИС

тел. +375 17 259 14 20;

правовые вопросы – тел. +375 17 259 14 09,

факс +375 17 373 91 66;

финансовые вопросы – тел. +375 17 259 14 04.

УНП 193002449, ОКПО 501297625000

IBAN BY09 MMBN 3012 0717 8001 0000 0000

в ОАО «Банк Дабрабыт»,

ул. Коммунистическая, 49, пом.1, 220002,

г. Минск, Республика Беларусь

BIC MMBNBY22

_____/

М.П.

_____ 2025 г.

_____/

М.П.

_____ 2025 г.

Спецификация

№	Наименование прав, срок действия прав	Кол- во	Цена без НДС, BYN	Стоимость без НДС, BYN	Сумма НДС, BYN	Всего с НДС, BYN
ИТОГО:						

* Срок действия прав _____ с даты _____.

Перечень технических требований

Программный комплекс сетевого экрана для защиты веб-приложений (далее – ПК) версии, имеющей действующий сертификат соответствия требованиям Технического регламента «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ), должен поставляться в комплекте с документацией в электронном или печатном виде на русском языке. Руководства по установке и администрации ПК.

Исполнитель должен передать Заказчику права на ПК, оказать техническую поддержку (гарантийное сопровождение) ПК, ввести его в эксплуатацию и обучить сотрудников Заказчика правилам эксплуатации ПК.

Состав ПК:

неисключительные права на основной узел системы управления;

неисключительные права на активные узлы анализа (до 1 000 запросов в секунду).

ПК лицензируется только в зависимости от реальной нагрузки на систему фильтрации веб трафика и позволяет Заказчику гибко изменять количество узлов фильтрации веб трафика без увеличения стоимости лицензии.

Исполнитель представляет детальное описание ПК в объеме и виде достаточном для понимания сотрудниками Заказчика. Описание и копии имеющейся технической документации на компоненты ПК предоставляются в электронном виде либо на электронном носителе информации.

Технические требования к программному комплексу

ПК необходим для создания эффективной системы защиты веб-приложений Заказчика от вредоносных воздействий из сети Интернет, а также обеспечения Заказчика инструментами для расследования подобных воздействий и предотвращения подобных инцидентов в будущем.

ПК должен быть установлен и функционировать под управлением операционной системы семейства Linux, которая распространяется под одной из открытых лицензий (GPL и т.п.) и должна находиться в стадии активной технической поддержки (выпускаться обновления, производиться закрытие обнаруженных уязвимостей и т.п.) на момент внедрения.

ПК должен состоять из следующих компонентов:

подсистемы захвата трафика, осуществляющей сбор трафика и его анализ различными способами;

подсистемы анализа трафика, осуществляющей поиск аномалий и реагирование (блокировку или предупреждение) в режиме реального времени;

подсистемы базы данных (БД), осуществляющей централизованный сбор, хранение и анализ данных транзакций с одной или нескольких подсистем захвата и анализа трафика, а также обеспечение централизованного хранения политик, правил и сигнатур;

подсистемы управления и мониторинга, обеспечивающей настройку общей для всей инсталляции политики информационной безопасности, мониторинг и аудит событий, а также подготовку отчетности через единый веб-интерфейс или REST API;

все компоненты системы должны обеспечивать возможность установки в инфраструктуре заказчика и функционирования без подключения к внешним, облачным сервисам.

Программное обеспечение ПК должно обеспечивать возможность установки каждого из компонентов ПК на отдельных виртуальных и физических сетевых узлах (узел захвата трафика, узел анализа, узел БД, узел управления) для создания распределенных масштабируемых и отказоустойчивых конфигураций.

ПК должен обеспечивать возможность:

одновременной работы нескольких узлов захвата и анализа трафика в активном режиме (active/active) с целью повышения масштабируемости и отказоустойчивости;

запуска нескольких модулей захвата и анализа трафика на одном физическом или виртуальном узле;

работы одновременно с несколькими защищаемыми приложениями (количество приложений не должно ограничиваться лицензионно), при этом подсистемы сбора и анализа трафика должны обладать способностью обслуживать различные группы защищаемых приложений;

поставки в виде дистрибутива программного обеспечения, установка которого возможна на виртуальные серверы Заказчика с индивидуальной конфигурацией;

установки подсистемы захвата трафика в контейнере Docker.

Поддержка программного обеспечения, виртуальных устройств должна осуществляться через службу технической поддержки производителя ПК.

Подсистемы сбора и анализа трафика должны поддерживать следующие режимы работы:

режим блокировки («в разрыв») – обратный прокси-сервер (reverse proxy);

режим мониторинга – анализ зеркалированного SPAN-трафика;

гибридный режим – одновременное использование режима блокировки и режима мониторинга на одном и том же узле анализа для различных приложений (например, мониторинг для тестирования и настройки, блокировки – продуктивного использования).

Режим блокировки («в разрыв») должен допускать возможность частичного или полного отключения блокировки на время настройки ПК, регламентных работ или нарушения функционирования ПК.

ПК должен:

обеспечивать возможность централизованного управления, а также сбора, анализа и хранения данных для нескольких узлов захвата и анализа трафика, каждый из которых может функционировать в одном из вышеперечисленных режимов;

иметь возможность терминирования защищенного SSL/TLS – трафика (SSL/TLS-offload), в том числе с размещением нескольких поддерживающих HTTPs веб-приложений (сайтов) на одном IP адресе, а затем упаковки обратно в SSL/TLS соединение;

поддерживать протокол WebSocket;

иметь функцию обработки массовых однотипных блокируемых запросов в специальном режиме непосредственно в подсистеме захвата трафика, без передачи в подсистему анализа трафика, для обеспечения оптимальной производительности при защите от бот-активности и DDoS атак или иной механизм реализации данной функции.

В общем виде требования к надежности ПК должны соответствовать требованиям по надежности, заданным в данном приложении или распорядительными документами Заказчика, в том числе и по, времени восстановления.

ПК должен обеспечивать возможность работы подсистем (узлов) в режиме Active/Active (с балансировкой нагрузки).

При использовании режима Active/Active для резервирования узлов захвата и анализа трафика, в случае сбоя одного из узлов, при котором он не способен обрабатывать трафик, перенаправление на работоспособные узлы должно осуществляться за счет внешнего балансировщика нагрузки.

ПК должен поддерживать режим, при котором в случае повышения нагрузки выше допустимой для имеющихся ресурсов серверов, на которых установлены компоненты ПК, часть запросов будет пропускаться далее к защищаемым приложениям без проверки, но проверка не будет отключена полностью и не произойдет отказ в обслуживании. Также должен обеспечиваться режим fail-open в случае сбоя одного или нескольких программных компонентов WAF.

ПК должен давать возможность устанавливать политику по умолчанию, на случай резкого увеличения нагрузки, сбоев или недоступности программных компонентов – «Пропустить», если для защищаемых приложений в приоритете доступность, либо «Заблокировать», если в приоритете безопасность.

ПК должен поддерживать возможность быстрого ручного отключения функции блокировки в интерфейсе управления, для каждого из защищаемых приложений, в случае сбоев или некорректной

настройки ПК.

Интерфейс управления должен обеспечивать версию каждой из выполненных настроек, чтобы в случае ошибок конфигурации, приведших к некорректной работе ПК, была возможность вернуться к одному из исходных состояний каждой из настроек.

Возможность восстановления ПК после сбоя должна обеспечиваться программными средствами архивирования и резервного копирования, рекомендуемыми разработчиками ПК.

ПК должен поддерживать круглосуточный режим функционирования. Допускается временная недоступность сервисов при проведении восстановительных (в случае сбоя) работ.

Программные и аппаратные компоненты ПК должны давать возможность проведения регламентных работ, работ по техническому обслуживанию, обновления программного обеспечения без перерыва сервиса.

При необходимости масштабирования (например, при недостатке производительности или изменении инфраструктуры доставки приложений Заказчика) ПК должен поддерживать добавление новых подсистем (узлов) или расширение ресурсов имеющихся узлов с распределением нагрузки без внесения изменений в код или архитектуру самого ПК и без прерывания в обслуживании;

При истечении срока действия технической поддержки, лицензии или превышении лицензионного лимита ПК не должен блокировать или прерывать трафик, а также снижать функциональность (пропускать трафик без анализа, прекращать блокировать потенциально-опасные, ограничивать настройки политики безопасности и т.п.).

Для обеспечения требуемого уровня защиты и эффективной эксплуатации, ПК должен иметь возможность интеграции с внешними системами, в частности:

- поддерживать взаимодействие с SIEM-системами;

- предоставлять возможность интеграции с другими системами с использованием механизмов syslog, SQL;

- предоставлять универсальный REST API для внешнего управления системой, который обеспечивает те же функции управления, что и штатный интерфейс управления;

- поддерживать функционал загрузки спецификации OpenAPI в качестве действий модели бизнес-логики;

- поддерживать мониторинг с использованием систем мониторинга Zabbix и Prometheus;

- предоставлять возможность интеграции со списками источников Threat Intelligence;

- иметь модуль интеграции со сканером защищенности веб-приложений и API для повышения качества выявления точек ввода данных (Data Entry Points) при сканировании и снижения воздействия сканера на анализируемое веб-приложение.

ПК должен обеспечивать защиту от следующих видов атак:

- атак на веб-приложения из перечня OWASP Top 10;

- атак на API из перечня OWASP Top 10 API Security Risks;

- атак на протокол HTTP, включая атаки на переполнение буфера;

- синтаксических атак в т.ч. различных атак класса injection (внедрение команд в передаваемые данные - SQL Injection, Code Injection, OS Command Injection, LDAP Injection, Path Traversal и др.);

- атак «методом грубой силы», в т.ч. переборных атак и атак класса «умный DoS»;

- логических атак на приложения, в том числе от атак на механизмы аутентификации и контроля сессий и атак на бизнес-логику;

- атак «внутри» передаваемых данных с произвольным уровнем вложенности (атаки на бэкенд, механизмы сериализации/десериализации и т.п.);

- атак на клиентов веб-приложений (CSRF, XSS и т.п.);

- 0-day и 1-day атак;

- атак с применением ботов и средств автоматизации Защита от нежелательной бот-активности.

ПК должен обеспечивать возможность контроля использования защищаемого приложения легитимными пользователями.

ПК должен поддерживать схемы работы «разрешено все, что не запрещено явно», «запрещено все, что не разрешено явно», а также комбинации обеих схем, в зависимости от рассматриваемой модели угроз и критичности защищаемых приложений.

ПК должен обеспечивать своевременное обнаружение факторов компрометации и возможность последующего расследования инцидентов.

ПК должен поддерживать следующие ключевые возможности:

- работу с использованием негативных методов обнаружения аномалий, в том числе:

- наличие базового набора встроенных сигнатур в комплекте поставки для защиты от угроз OWASP top 10;

- поддержка распространенного открытого формата веб-сигнатур ModSecurity;

создание аномальных последовательностей (цепочек) действий, для моделирования нежелательного поведения.

работу на основе нормальных моделей работы приложения (позитивных моделей):

возможность гибкой настройки различных типов моделей для каждого из защищаемых приложений, в том числе:

модели определения и фильтрации статического контента;

модели валидации протокола HTTP, включая контроль заголовков, cookie и др.;

рекурсивной модели синтаксического анализа запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности данных (в частности, XML, JSON, BASE64, GZIP, SOAP, Zstd, Brotli, Protocol Buffers);

модели проверки соответствия XML-подобных форматов данных заданным схемам XSD, загружаемым в виде файлов в интерфейсе WAF;

модели источников – определение характеристик источника на основе параметров запроса;

модели определения логических действий (бизнес-действий) в приложении, параметров логических действий и их значений, последовательностей действий, проверки успешности действий;

модели идентификации, аутентификации и контроля сессий в приложении;

модели защиты от переборных атак и атак типа «умный DoS» на уровне отдельных логических действий и произвольных параметров действия.

наличие готовых моделей валидации протокола HTTP и синтаксического анализа запросов для типового веб-приложения в комплекте поставки;

возможность ручной тонкой настройки моделей отдельно для каждого из логических действий и параметров, в частности настройка сигнатурного анализа, моделей параметров, конфигураций модуля защиты от переборных атак.

противодействие переборным атакам:

возможность ограничения количества запросов, направляемых приложению в единицу времени;

возможность индивидуальной настройки параметров противодействия переборным атакам для отдельных логических действий в приложении;

детектирование бот-активности по аномальному превышению медианного времени задержки ответа веб-приложения по сравнению с историческими данными или иной механизма реализации данной функции;

возможность блокировки периодических однотипных запросов от одного источника;

возможность блокировки явных переборов любых параметров запроса.

обнаружение аномалий и значимых событий:

возможность обнаружения аномалий или значимых данных как в HTTP-запросах, так и в HTTP-ответах;

возможность обнаружения аномалий работы приложения на основе сопоставления значений параметров HTTP запросов/ответов с сигнатурами атак или иной механизм реализации данной функции;

возможность обнаружения аномалий или значимых данных в работе приложения на основе настроенных позитивных моделей приложения (совпадение с моделью или наоборот – отклонение от нее);

обнаружение аномалий и значимых параметров непосредственно внутри вложенных данных, передаваемых по протоколу HTTP без ограничений на количество уровней вложенности или иной механизм реализации данной функции;

возможность обнаружения аномалий, свидетельствующих о возможных попытках атак, осуществляемых «методом грубой силы» (bruteforce);

возможность обнаружения аномалий или значимых данных в процессе работы механизмов идентификации, аутентификации, авторизации пользователей и контроля пользовательских сессий;

возможность обнаружения аномалий нарушения бизнес-логики приложения или контроля выполнения бизнес-логики путем использования соответствующей позитивной модели работы приложения;

контроль страновой принадлежности источника в соответствии с автоматически обновляемой базой GeoIP.

подавление ложных срабатываний и оптимизация отображения информации:

наличие механизма предварительного («раннего») подавления ложных срабатываний, чтобы исключить возможность их влияния на сформированные правила принятия решений, а также чтобы предотвратить их попадание в интерфейс мониторинга;

наличие функции упрощенного («быстрого») подавления ложных срабатываний оператором Системы непосредственно при просмотре описания выявленной аномалии;

возможность тонкой настройки подавления ложных срабатываний различных механизмов определения аномалий в привязке к отдельным параметрам запроса/ответа или логическим действиям в

приложении или иной механизм реализации данной функции;

возможность разделения запросов к статическому и динамическому контенту с отдельным режимом обработки статического контента для экономии системных ресурсов и минимизации времени обработки статического контента.

принятие решений:

наличие настраиваемого модуля принятия решений, позволяющего выделять значимые события информационной безопасности и принимать решения относительно дальнейших действий в отношении HTTP-транзакций (запрос/ответ);

управление правилами принятия решений на основе данных об источнике IP адрес, пользователь, ID сессии) и цели HTTP-транзакции (приложение, логическое (бизнес)-действие), а также обнаруженных в ней аномалиях или значимых данных;

поддержка следующих возможных решений: заблокировать HTTP-транзакцию, пропустить HTTP-транзакцию, пометить HTTP-транзакцию, модифицировать ответ;

управление правилами принятия решений (создание, удаление, перегруппировка) с помощью графического конфигулятора через интерфейс управления.

ПК должен поддерживать гибкие механизмы автоматического обучения для снижения затрат времени и ресурсов на настройку ПК при внедрении и обслуживании, в том числе, в условиях частых изменений функционала защищаемых приложений, а также в условиях активного цикла разработки.

ПК должен обладать следующими возможностями автоматического обучения:

автоматическое определение и описание статического контента на основе анализа статистики запросов к защищаемым приложениям;

автоматическое построение рекурсивной модели синтаксического анализа данных запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности (в частности, XML, JSON, BASE64, GZIP, SOAP, Zstd, Brotli, Protocol Buffers);

автоматическое построение модели маршрутизации запросов для веб-приложения;

автоматическое построение моделей логических действий в приложении и моделей параметров этих действий, а также последовательностей (цепочек) логических действий или иной механизм реализации данной функции;

оценка отклонения параметров логических действий в веб-приложении от статистической нормы;

автоматическая настройка порогов срабатывания модуля противодействия переборным атакам и медленным ботам, анализирующего частоту запросов на конкретный URL или к конкретной функции веб-приложения.

ПК должен иметь следующие возможности по выполнению автоматического обучения:

непрерывное обучение в процессе функционирования;

периодический запуск заданий по обучению по установленному расписанию;

ручной однократный запуск заданий по обучению.

Результаты автоматического обучения должны быть полностью интерпретируемыми и корректируемы администратором ПК.

ПК должен обеспечивать возможность инкрементного обучения (только для изменений, произошедших с момента предыдущего обучения), а также частичной ручной корректировки результатов обучения для отдельных статических ресурсов, элементов модели синтаксического анализа, логических действий и т.п. без необходимости проводить полное обучение заново или иной механизм реализации данной функции.

ПК должен обеспечивать централизованное управление компонентами с использованием единого веб-интерфейса.

Функции управления ПК должны включать:

управление по протоколу HTTP или HTTPS с использованием специализированного веб-интерфейса, либо с использованием защищенного протокола SSH (только для системного администрирования);

управление политиками безопасности (правилами реагирования, настройками моделей нормального функционирования приложений, заданиями по автоматическому обучению) с использованием только графического интерфейса (чтобы данную задачу могли выполнять пользователи с ролью Аналитик, не обладающие навыками системного администрирования и работы с командной строкой);

редактирование конфигурации подсистемы захвата трафика (обратный-прокси) с использованием графического интерфейса;

возможность загрузки SSL-сертификатов в графическом интерфейсе ПК;

управление с использованием REST API, в целях интеграции с другими решениями;

возможность мониторинга и управления конфигурациями для нескольких защищаемых приложений из общего интерфейса;

возможность отображения текущего статуса и управления конфигурациями нескольких узлов анализа, функционирующих в различных режимах с различными наборами защищаемыми приложениями;

возможность создания политик безопасности (правил), распространяющихся на отдельные приложения, группы приложений или все защищаемые приложения одновременно;

возможность оператору создавать и запускать задания на автоматическое обучение, а затем вручную редактировать любые модели и результаты работы механизмов автоматического обучения, непосредственно в веб-интерфейсе управления.

ПК должен обеспечивать следующие функции безопасности управления:

поддержку механизма идентификации и аутентификации пользователей на основе имени пользователя и пароля;

возможность настройки из интерфейса парольных политик, в том числе:

-минимальную длину пароля;

- необходимость использования цифр, специальных символов, строчных и заглавных букв;

- время жизни пароля;

поддержку двухфакторной аутентификации с Time-Based OTP (TOTP) в качестве второго фактора;

поддержку авторизации пользователей на основе ролевой модели, которая предусматривать разграничение доступа для трех типов ролей:

администратор – имеет доступ ко всем функциям управления, в том числе, к настройкам политики информационной безопасности и системным настройкам;

аналитик – имеет доступ только к настройкам политики информационной безопасности и не имеет возможности менять системные настройки;

дежурный администратор – имеет доступ к разделу мониторинга и информации о событиях информационной безопасности только на чтение и не имеет возможности изменять настройки ПК.

возможность назначать пользователям права в рамках ролевой модели (аналитик, администратор, дежурный администратор) на основе LDAP-фильтров;

аудит действий пользователей в интерфейсе, в том числе – кто выполнил действие, тип действия и произошедшие изменения по сравнению с предыдущим состоянием;

версионность конфигурационных настроек системы: в т.ч. базовых конфигурационных настроек, настроек модулей анализа, моделей нормального функционирования приложений, правил принятия решений, версионность должна обеспечиваться отдельно для всех перечисленных типов объектов конфигурации или иной механизм реализации данной функции.

Функции централизованного мониторинга и аудита ПК должны включать:

вывод обобщенной статистики по следующим параметрам: статусы HTTP ответа сервера, текущей пропускной способности (входящий/исходящий трафик), задержки обработки запросов приложением, уровня враждебности среды;

вывод в агрегированном виде сообщений об обнаруженных и/или заблокированных атаках на приложения и других аномальных событиях. Агрегация должна происходить по источникам запросов, приложениям и отдельным действиям в них, типам обнаруженных аномалий и времени возникновения аномалий;

агрегирование информации об источниках аномальных запросов по географическому распределению источников по странам, по номерам автономных систем;

оповещение пользователей системы о событиях безопасности с использованием электронной почты, гибкая настройка оповещений через веб-интерфейс управления;

возможность независимой для каждого приложения настройки глубины хранения для трех типов данных – всех транзакций (пар HTTP-запрос/ответ), аномальных (подозрительных) транзакций и событий безопасности, а также возможность настройки записи ответов или иной механизм реализации данной функции или иной механизм реализации данной функции;

возможность настройки выгрузки данных по отдельным заданным логическим действиям;

возможность автоматической генерации отчетов в формате PDF, содержащих статистику событий информационной безопасности за заданные промежутки времени, в том числе периодические отчеты с периодичностью «раз в сутки», «раз в неделю», «раз в месяц»;

запись лог-файлов в формате Syslog с гибкой настройкой записываемых данных (настраиваемый формат лог-файлов);

функции мониторинга, поддерживаемые при интеграции с внешними системами должны включать:

возможность передачи данных в режиме реального времени в систему мониторинга и корреляции

событий информационной безопасности (SIEM);

наличие схемы для передачи данных о состоянии физических и программных компонентов Системы (процессор, память, пространство на накопителях данных, состояние процессов, БД и т.п.) в инструмент для мониторинга Zabbix.

Исполнитель:	Заказчик:
« ____ » _____ 2025 г.	« ____ » _____ 2025 г.

прохождение обучения.

По результатам ввода ПК в эксплуатацию должен быть разработан следующий комплект документов:

Акт передачи прав на программное обеспечение.

Схемы, согласованные с Заказчиком до ввода ПК в эксплуатацию.

Руководства по установке и администрации ПК.

Акт ввода ПК в эксплуатацию.

Исполнитель: « ____ » _____ 2025 г.	Заказчик: « ____ » _____ 2025 г.
--	---

Параметры технической поддержки программного комплекса

Техническая поддержка (гарантийные обязательства) включают услуги, которые оказываются Заказчику на постоянной основе на весь срок действия технической поддержки (гарантийных обязательств) сроком 13 месяцев с даты ввода ПК в эксплуатацию.

Исполнитель должен обеспечить следующие общие условия сопровождения ПК:

наличие выделенной линии службы приема и разрешения технических запросов (заявок) по телефону, e-mail и/или мессенджер и/или с использованием системы ServiceDesk;

прием обращений в службу технической поддержки должен осуществляться по телефону в рабочие дни с 08:30 по 17:30 и в круглосуточном режиме (24x7) по e-mail и/или мессенджер и/или с использованием системы Service desk;

количество одновременно обрабатываемых запросов (с гарантированным уровнем SLA) в службе поддержки не менее 1, все запросы поступают от технических специалистов Заказчика;

возможность удаленного подключения специалистов Исполнителя для консультации специалистов Заказчика в формате видеоконференцсвязи;

способ оказания услуг: удаленно, на русском языке;

количество защищаемых приложений Заказчика, для которых должно осуществляться сопровождение – не менее 4.

Процедура обслуживания запроса:

Открытие запроса осуществляется Заказчиком в режиме 24x7 (и/или по электронной почте, и/или мессенджер и/или с использованием системы Service desk).

При обращении Заказчик определяет приоритет Запроса. При обработке специалист Исполнителя может менять приоритет, если в запросе участвуют Сервисы, которые не соответствуют указанному приоритету или запрос не соответствует описанию критичности.

Время оказания услуг считается со времени регистрации запроса до его закрытия.

Оказание услуг осуществляется в соответствии с параметрами, указанными в таблице №1.

Таблица № 1

Приоритет	Время реакции	Продолжительность решения проблемы	Периодичность информирования заказчика о ходе решения проблемы
Приоритет 1. Критично	≤ 30 мин	не более 6 часов*	1 раз в час
Приоритет 2. Срочно	≤ 1 часа	не более 8 часов	1 раз в 3 часа
Приоритет 3. Некритично	≤ 4 рабочих часов	не более 3 рабочих дней	по запросу Заказчика и по факту решения проблемы
Приоритет 4. Консультация	Следующий рабочий день	не учитывается	по запросу Заказчика

*Время корректируется по итогам выбора исполнителя услуги, согласно предложениям участников.

Оценка приоритета осуществляется согласно таблице № 2.

Таблица № 2

Приоритет	Описание
Критично	Сбой непосредственно влияет на работу компании и несет экономические потери для компании
Срочно	Сбой непосредственно влияет на работу компании и/или может привести к экономическим и репутационным рискам.
Некритично/Консультация	Сбой, который влияет на работу компании, но не влияет на экономические или репутационные риски.

В случае аварийной ситуации со статусом «Критично» Исполнитель должен иметь возможность в

