FACILITY SECURITY REQUIREMENTS

TAPA
Transported Asset Protection Association

Transported Asset Protection Association

Регламент Безопасности Объектов РБО 2020

Стандарты TAPA

TAPA Северная и Южная Америка
5030 Champion Blvd, G-11 #266 Boca Raton, Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Азиатско-Тихоокеанский регион
1 Gateway Drive, Westgate Tower #07-01,
Singapore 608531
www.tapa-apac.org
Tel. (65) 66844687

TAPA Европа, Ближний Восток и Африка
Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
The Netherlands
www.tapaemea.org
Tel. +44 1633 251325

Оглавление

Оглавление (продолжение)

□□□

1. Введение

1.1 Предназначение настоящего документа РБО

Настоящий документ «Регламент Безопасности Объектов» (РБО) является официальным стандартом TAPA по безопасности складских услуг и услуг хранения. Это признанный глобальный стандарт, применимый к коммерческим соглашениям и контрактам между Заказчиками и Поставщиками Логистических Услуг (далее - ПЛУ) и/или иными Заявителями, желающими пройти сертификацию.

Разрабатывая данный Стандарт, Ассоциация TAPA учитывает существующие многочисленные различия и особенности в предоставлении услуг хранения на глобальном, региональном и даже внутрикорпоративном уровнях, а также возможность применения РБО как ко всему объёму, так и к части услуг, предоставляемых ПЛУ/Заявителями. В зависимости от сложности и масштабов операций в цепях поставок, сертификация по стандартам TAPA может проходить как в отношении одного, так и нескольких ПЛУ/Заявителей и их субподрядчиков, прошедших квалификационный отбор.

Область применения

ТАПА разработала три варианта проведения сертификации:

- Сертификация одиночного объекта Независимым Органом Аудита (НОА).
- Одновременная сертификация нескольких объектов НОА.
- Самостоятельная сертификация Уполномоченным Аудитором (УА) ПЛУ/Заявителя или НОА.

Целевая аудитория

Стандарты TAPA обычно внедряются и используются:

- Заказчиками
- ПЛУ/Заявителями
- Правоохранительными органами или иными государственными структурами
- Профессиональными организациями в области цепей поставок
- Страховыми компаниями

1. Введение

1.2 Ресурсы для внедрения РБО TAPA

Внедрение стандарта РБО является ответственностью ПЛУ/Заявителя и осуществляется за счёт его средств, если иное не оговорено в контракте между Заказчиком и ПЛУ/Заявителем.

1.3 Защита и конфиденциальность политик и процедур Поставщиков

Копии документированных политик и процедур по безопасности ПЛУ/Заявителя предоставляются Заказчику в соответствии с подписанным соглашением о неразглашении между ПЛУ/Заявителем и Заказчиком, при обращении с ними должны применяться принципы конфиденциальности.

2. Об ассоциации TAPA

2.1 Цели ассоциации TAPA

Хищение грузов – один из главных вызовов безопасности в цепях поставок производителей дорогостоящей, высоколиквидной продукции и их поставщиков логистических услуг.

Угрозу сегодня представляют не столько отдельные случаи хищений. Напротив, это является результатом целенаправленной и скоординированной деятельности организованных преступных групп, действующих на международном уровне и использующих в достижении своих целей постоянно совершенствующиеся способы нападений на объекты хранения, транспортные средства и персонал.

TAPA это уникальный форум, объединяющий мировых производителей, поставщиков логистических услуг, экспедиторские и транспортные компании, правоохранительные органы и прочие заинтересованные стороны в интересах снижения потерь в международных цепях поставок. Своей основной целью TAPA видит предотвращение хищений через использование актуальной информации о текущих угрозах и внедрения эффективных мер превентивного контроля.

2.2 Миссия TAPA

Миссия TAPA – способствовать защите активов своих членов через снижение потерь грузов в цепях поставок. TAPA достигает этого путём разработки и внедрения единых стандартов безопасности, наилучших практик, технологий, обучения, анализа и оценки рисков, сотрудничества в сфере регулирования отрасли, а также через реализацию превентивных защитных мер и проактивного выявления криминальных угроз в цепях поставок.

3. Стандарты TAPA

3.1 Стандарты безопасности TAPA

В целях обеспечения безопасности транспортировки и хранения грузов повышенной категории риска (ПКР) TAPA разработала следующие международные стандарты безопасности:

- Регламент безопасности объектов (РБО) — минимальный набор требований для безопасного хранения на складах или объектах временного хранения в цепи поставок.
- Регламент безопасности грузоперевозок (РБГ) ориентирован на грузоперевозки автотранспортом и представляет собой минимальный набор требований по безопасности при наземной доставке грузов автомобильным транспортом в цепи поставок.

Международные стандарты TAPA пересматриваются и по мере необходимости обновляются каждые три года.

Настоящий документ содержит только требования РБО.

- Процесс сертификации РБО прописан в отдельном документе - Рамочном документе по сертификации РБО TAPA
- Оба документа – текущая версия Требований РБО и Рамочный документ по сертификации РБО должны использоваться для прохождения сертификации.

3.2 Внедрение стандартов

Успех при внедрении стандартов безопасности TAPA зависит от уровня взаимодействия ПЛУ (Поставщиков логистических услуг)/Заявителей, Заказчиков (Грузовладельцев) и Уполномоченных аудиторов TAPA.

4. Правовые основы

4.1 Область применения

РБО – это всеобъемлющий международный стандарт, все разделы которого носят обязательный характер, за исключением случаев, когда предоставляется официальное освобождение от требований. (См. Раздел 6).

4.2 Перевод стандартов

Там, где английский язык не является основным, и в определенных случаях требуется перевод, в обязанности ПЛУ/Заявителя и его уполномоченных лиц входит обеспечение перевода всего Регламента или его частей на официальные языки, что отражает намерения TAPA по более широкому внедрению и популяризации своих стандартов.

4.3 Бренд “TAPA”

«TAPA» является зарегистрированным торговым знаком Ассоциации по защите перевозимых грузов (TAPA) и не может быть использован без предварительного письменного согласия TAPA, полученного от её официальных представителей в соответствующих регионах. Стандарты TAPA и связанные с ними материалы публикуются силами TAPA и не могут быть пересмотрены, отредактированы или изменены какой-либо из сторон без предварительного письменного разрешения TAPA. Злоупотребление брендом TAPA может привести к отзыву сертификата или последствиям юридического характера.

4.4 Ограничение ответственности

Публикуя данные стандарты, TAPA не несёт ответственности и не предоставляет никаких гарантий того, что вне зависимости от того, были ли требования стандартов полностью выполнены и должным образом внедрены, все случаи утраты грузов впредь будут исключены. Любая ответственность за кражи или утрату грузов при хранении, согласно стандарту РБО, возлагается на ПЛУ/Заявителя и/или Заказчика в соответствии с положениями и условиями, прописанными в заключенном между ними контракте, и законодательными нормами, применяемыми в пределах местной юрисдикции.

5. Контракты и субподряд

5.1 Контрактные обязательства

ПЛУ/Заявитель, его уполномоченные агенты и субподрядчики отвечают за безопасность и качество транспортировки, хранения и обращения с имуществом Заказчика на протяжении всего цикла ответственности, включая приём груза, перевозку, временное хранение и доставку согласно условиям поставки или договору.

Если в договор между ПЛУ/Заявителем и Заказчиком включена ссылка на стандарт РБО, это также должно быть отражено в программе безопасности ПЛУ/Заявителя.

ПЛУ/Заявитель должен представить Заказчику подтверждение сертификации по стандарту РБО и, в зависимости от обстоятельств, документальные доказательства соответствия требованиям РБО. Кроме того, любое предполагаемое несоответствие ПЛУ/Заявителя требованиям РБО должно регулироваться условиями контракта, заключенного между Заказчиком и ПЛУ/Заявителем.

5.2 Привлечение третьих лиц (субподряд)

Привлечение третьих лиц (субподрядчиков) к оказанию услуг хранения должно включать договорное требование о том, что субподрядная организация ПЛУ/Заявителя соответствует всем требованиям РБО.

5.3 Расследование случаев несоответствия и разрешение споров TAPA

В случае получения официальной жалобы на деятельность сертифицированного ПЛУ/Заявителя, ассоциация TAPA (после проведения расследования и подтверждения фактов несоответствия) может потребовать от ПЛУ/Заявителя заключения договора на повторный аудит за счёт ПЛУ/Заявителя. Если ПЛУ/Заявитель не проходит аудит или отказывается следовать данному требованию, его сертификат может быть отозван.

6. Освобождение от требований

6.1 Общие положения

Освобождение от требований – это письменное подтверждение, которое выдается либо с целью полностью освободить объект от выполнения определенного требования стандарта TAPA или одобрить альтернативные меры для соблюдения требований. Освобождение от требований запрашивается в том случае, если ПЛУ/Заявитель по объективным причинам не может обеспечить соответствие определенному требованию РБО, но способен обосновать альтернативные меры безопасности. Освобождение от требований действует в течение всего периода сертификации.

Все запросы об освобождении от требований (частичном или полном) по конкретному требованию РБГ ПЛУ/заявитель должен подавать в Независимый Орган Аудита (НОА)/Уполномоченному Аудитору (УА) по установленной форме TAPA (доступна на веб-сайте TAPA). ПЛУ/Заявитель несёт полную ответственность за точность и достоверность информации, указанной в запросе на освобождение.

Каждый полученный запрос на освобождение от требований НОА/УА направляет на утверждение в Региональный комитет TAPA по освобождению от требований. НОА/УА отвечает за полноту указанных в запросе сведений и оценивает целесообразность его направления в TAPA; что включает проверку эффективности компенсирующих мер и/или альтернативных способов обеспечения безопасности.

При возникновении у официальных представителей TAPA и/или Заказчика достаточных оснований полагать, что условия для предоставления освобождения от требований изменились, TAPA проводит официальное рассмотрение. При этом ПЛУ/Заявитель должен учитывать, что по результатам данного рассмотрения TAPA может отозвать освобождение от требований.

6.2 Процедура освобождения от требований

Если ПЛУ по объективным причинам не может выполнить определенное требование РБО, запускается процесс освобождения от требований, приведенный ниже.

Таблица 1: Ответственность сторон при подаче и обработке запроса

Шаг	Ответственность	Мероприятия
1.	ПЛУ/Заявитель	Определяет и обосновывает меры по снижению рисков.
2.	ПЛУ/Заявитель	Заполняет форму запроса на освобождение от требований TAPA и направляет ее НОА/УА
3.	НОА/УА	Рассматривает и проверяет полноту информации в форме запроса ПЛУ/Заявителя на освобождение от требования TAPA.

Шаг	Ответственность	Мероприятия
4.	НОА/УА	Направляет форму запроса на освобождение от требования в Региональный комитет TAPA по освобождению от требований.
5.	Региональный комитет TAPA по освобождению от требований	Рассматривает запрос и, либо предоставляет освобождение от требований, либо отказывает в его предоставлении.

Если в освобождении от требований отказано

Если Региональный комитет TAPA по освобождению от требований не согласует запрос на освобождение от требования, то ПЛУ/Заявитель обязан выполнить требования безопасности РБО в полном объеме.

Если освобождение от требований одобрено

Если Региональный комитет TAPA по освобождению от требований согласует запрос на освобождение от требований, стороны предпринимают следующие шаги:

Таблица 2: Процедура одобрения освобождения от требований

Шаг	Ответственность	Мероприятия
1.	Региональный комитет TAPA по освобождению от требований	Документально закрепляет указанные в освобождении от требования детали.
2.	Региональный комитет TAPA по освобождению от требований	Указывает срок действия освобождения от требования (максимум до трех лет) и отправляет копию УА.
3.	УА	Уведомляет ПЛУ/Заявителя о результатах рассмотрения запроса на освобождение от требования.
4.	ПЛУ/Заявитель	Выполняет условия освобождения от требования. В случае неспособности выполнить указанные условия, освобождение от требований утрачивает силу.

6. Освобождение от требований

6.3 Освобождение от требований для физического ограждения и закрытых зон хранения товаров повышенной категории риска (ЗЗХ)

TAPA рассматривает возможность освобождения от всех или от части требований к физическому ограждению и/или ЗЗХ, только в случае соблюдения всех указанных ниже условий:

Общие положения:

- Запрос на освобождение от требований подан в соответствии с утвержденным TAPA регламентом и поддерживается НОА/УА.
- Запрос на освобождение от требования включает подробное описание мер по снижению рисков для обеспечения того, что товарно-материальные ценности в процессе хранения не подвергаются необоснованному риску утраты или хищения.
- Одновременно с подачей запроса об освобождении от требований должна быть проведена и предоставлена оценка рисков. Любые значительные уязвимости, выявленные в ходе оценки рисков, должны быть отдельно перечислены в запросе, а также указаны меры по снижению указанных рисков до приемлемого уровня.

Меры, которые применяются и документируются при подаче запроса на освобождение от требований:

- **Физическое ограждение:**
  - Дополнительное оборудование, ресурсы и процедуры, которые внедрены для возможности своевременного обнаружения несанкционированного проникновения на объект посторонних лиц и транспортных средств, должны предусматривать, но не ограничиваться, установкой дополнительного освещения, покрытия системой видеонаблюдения, усиленными процедурами в отношение проверки документов физических лиц и транспортных средств, определение зон, где нахождение персонала разрешено только в униформе или сигнальных жилетах.
  - По периметру должны быть установлены указатели с надписями на местном языке «Посторонним вход запрещен», «Парковка только для персонала».
  - Указатели на внешней стороне погрузочных доков или стенах здания с предписанием для водителей, посетителей и т.д. следовать к бюро пропусков или установленному месту приёма посетителей.
  - Подтверждение того, что на объекте внедрены процедуры, обеспечивающие проведение регулярных еженедельных

инспекций внешней зоны погрузки склада на соответствие условиям, согласованным в освобождении от требований.

- **Закрытые зоны хранения ТПКР:**
  - Для предоставления освобождения от требований для закрытых зон хранения товаров ПКР (в случае, где они не предусмотрены) в ежегодной оценке рисков должны быть предложены и задокументированы меры по снижению рисков.
  - К запросу на освобождение от требований должна прилагаться декларация, подписанная ПЛУ/Заявителем, о том, что ни один из его Заказчиков не требует наличия на объекте закрытой зоны хранения товаров ПКР.

7. Требования по безопасности

Раздел	Общие требования:	A	B	C
7.0				
7.0.1	Все политики и процедуры, предусмотренные настоящим стандартом, должны быть задокументированы.	✔	✔	✔
7.0.2	В отношение ключей от дверей, замков и электронных карт доступа необходимо наличие процедуры, журнала учёта выдачи и/или плана использования, которые позволяют осуществлять контроль за физическими и электронными ключами.	✔	✔	✔

Раздел	Внешний периметр	A	B	C
7.1				
Внутренняя территория объекта, зона погрузки и выгрузки (общие требования)				
7.1.1	Система видеонаблюдения позволяет отслеживать перемещение во внешней зоне разгрузки и погрузки (включая точки входа и выхода персонала), обеспечивая непрерывную идентификацию всех транспортных средств и персонала, за исключением тех периодов, когда видеонаблюдение затруднено в связи с текущей операционной деятельностью (например, текущая загрузка или разгрузка транспортного средства).	✔	✔	
7.1.2	Зоны погрузки и разгрузки должны иметь достаточную освещенность. *Примечание: Освещение может быть постоянным, а также с активацией по сигналу датчиков движения, звука и т. п., с возможностью немедленного включения освещения.*	✔	✔	✔
7.1.3	Утвержденные процедуры описывают порядок действий в случае обнаружения посторонних лиц и транспортных средств на внешней территории объекта, включая зоны погрузки и разгрузки. Процедуры доводятся до соответствующего штатного персонала и сотрудников охранных организаций.	✔	✔	✔
7.1.4	Внутренний периметр объекта, зоны разгрузки и погрузки контролируются надлежащим образом с целью предотвращения несанкционированного доступа третьих лиц.		✔	✔
7.1.5	Окна и проёмы, расположенные на уровне поверхности земли, а также ворота грузовых доков должны быть защищены противотаранными барьерами в случае, если результаты ежегодной оценки рисков на объекте свидетельствуют о необходимости внедрения данной меры (см. «Оценка рисков», раздел 7.6.5.)	✔		
Физическое ограждение				
7.1.6	Физическое ограждение обеспечивает защиту внутренней территории объекта, зон разгрузки и погрузки.	✔		

Раздел	Внешний периметр	A	B	C
7.1.7	Минимальная высота физического ограждения (забора) на объекте, включая зоны погрузки и выгрузки - 1,8 метра (6 футов). *Примечание: физическое ограждение (забор), предназначенное для предотвращения несанкционированного доступа третьих лиц, должно иметь высоту 1,8 метра по всей протяженности, включая зоны, где имеются перепады высот, например, уровень земли ниже.*	✔		
7.1.8	Физическое ограждение (забор) по периметру объекта, зон погрузки и выгрузки содержится в исправном состоянии.	✔		
7.1.9	Ворота внешнего периметра, вокруг внутреннего двора, зон погрузки и выгрузки контролируются сотрудниками охраны или техническими средствами.	✔		
7.1.10	Целостность физического ограждения объекта проверяется на предмет возможных повреждений как минимум раз в неделю.	✔		
Внешняя зона грузовых доков				
7.1.11	Внешняя зона грузовых доков просматривается цветными камерами видеонаблюдения или камерами, работающими в режиме «день/ночь».	✔	✔	✔
7.1.12	Камеры установлены таким образом, чтобы обеспечить наблюдение за операционной деятельностью и перемещениями персонала во внешней погрузочно-разгрузочной зоне доков, за исключением тех периодов, когда обзор камерами затруднён в связи с текущей операционной деятельностью (например, загрузка и разгрузка транспортного средства).	✔	✔	✔
7.1.13	Все транспортные средства и физические лица во внешней зоне погрузочных доков всегда должны быть хорошо различимы.	✔		
7.1.14	Транспортные средства и физические лица во внешней зоне грузовых доков должны быть различимы в большинстве случаев.		✔	✔
7.1.15	Внешняя сторона вокруг ворот грузовых доков должна иметь достаточное освещение.	✔	✔	✔
Допуск личного транспорта на внутреннюю территорию объекта				
7.1.16	Доступ для личных транспортных средств внутрь периметра объекта предоставляется только при условии предварительного согласования и ограничен местами, обозначенными соответствующими указателями. Парковка личного транспорта в радиусе 25 метров от ворот грузовых доков запрещена. Процедуры использования и согласования мест парковки на территории объекта закреплены документально.	✔	✔	✔

Раздел	Внешние стены, крыша и двери	A	B	C
7.2				
Внешние стены здания: Система видеонаблюдения				
7.2.1	Цветные или работающие в режиме «день/ночь» камеры видеонаблюдения обеспечивают обзор всех внешних сторон здания.	✔		

Раздел	Внешние стены, крыша и двери	A	B	C
7.2.2	Цветные или работающие в режиме «день/ночь» камеры видеонаблюдения обеспечивают обзор всех внешних сторон здания, на которых имеются двери, окна и другие проёмы.		✔	
7.2.3	Область покрытия внешних камер видеонаблюдения обеспечивает непрерывную идентификацию всех транспортных средств и персонала за исключением тех периодов, когда обзор затруднен в связи с текущей операционной деятельностью (например, загрузка или разгрузка транспортного средства).	✔		
7.2.4	Все транспортные средства и физические лица хорошо различимы камерами видеонаблюдения, расположенными снаружи.	✔		
7.2.5	Камеры видеонаблюдения, расположенные снаружи, позволяют различать транспортные средства и физические лица в большинстве случаев.		✔	
Внешние стены и крыша				
7.2.6	Внешние стены и крыша спроектированы и выполнены с использованием прочных материалов, препятствующих проникновению (например, из кирпича, блоков, сборных бетонных плит, сэндвич-панелей).	✔	✔	✔
7.2.7	Любое открывающееся окно, вентиляционный люк или иной другой проём на внешних стенах здания, а также глухие окна, расположенные ниже, чем 3 метра от поверхности, должны быть снабжены физическим ограждением или датчиками охранной сигнализации, подключенными к основному пульту охраны объекта.	✔	✔	
7.2.8	Любое открывающееся окно, оконный проём дневного света, вентиляционный люк или иной проём в конструкции крыши, должен иметь физическое ограждение **или** оснащен датчиками охранной сигнализации.	✔		
7.2.9	Внешний доступ на крышу (пожарная или маршевая лестница) должен быть: Физически заблокирован и просматриваться системой видеонаблюдения (цветные или работающия в режиме «день/ночь» камеры) **или** Физически заблокирован и оснащен датчиками охранной сигнализации.	✔		
7.2.10	Внешний доступ на крышу (пожарная лестница или маршевая лестница) должен быть заблокирован.		✔	✔
7.2.11	Все двери по внешнему периметру здания и офисные двери оборудованы датчиками охранной сигнализации для обнаружения несанкционированного доступа и выведены на основной пульт охраны. *Примечание: Ворота грузовых доков не подпадают под данное требование. См. п.7.2.17 по требованиям сигнализации для дверей грузовых доков.*	✔	✔	✔
7.2.12	Каждая внешняя дверь, проход в офисную часть или другой проём должны иметь уникальный идентификатор и индивидуально или зонально обозначены в системе охранной сигнализации объекта.	✔		

Раздел	Внешние стены, крыша и двери	A	B	C
7.2.13	Все двери внешнего периметра здания должны быть всегда заперты и защищены за исключением периодов их активного использования. Контроль осуществляется с помощью ключей/кодовых замков.	✔	✔	
7.2.14	Двери и дверные проёмы для прохода персонала должны быть надежно защищены от взлома и проникновения. Если дверные петли расположены снаружи, они должны быть укреплены заклепками или заварены. Использование дверей из стекла запрещено, если на них не установлены датчики разбития или иные технические средства сигнализации (например, устройство сигнализации с инфракрасным пассивным датчиком) с выводом тревоги на пульт охраны или оборудованы решетками/сетками.	✔	✔	✔
7.2.15	Аварийные выходы используются исключительно в чрезвычайных ситуациях для эвакуации персонала (например, пожарные выходы), находятся под сигнализацией и оборудованы системой звукового оповещения в случае вскрытия по индивидуальному или зональному принципу.	✔	✔	
7.2.16	Все ворота грузовых доков имеют надежную конструкцию, способную предотвратить и/или затруднить проникновение на объект с использованием подручных средств и переносных механических инструментов.	✔	✔	✔
7.2.17	**Ворота грузовых доков** **Нерабочее время:** Ворота грузовых доков закрыты и заблокированы (обесточены или механически заблокированы). Ворота грузовых доков поставлены на сигнализацию для обнаружения проникновения с выводом тревожного сигнала на основной пульт охраны. **Рабочее время:** Двери грузовых доков должны быть закрыты за исключением периодов активного использования. Ворота доков, выполненные в виде складывающейся двери-створки, должны быть снабжены механической защелкой/щеколдой и быть минимум 2,4 метра (8 футов) в высоту.	✔	✔	✔

Раздел	Входные группы офиса и склада	A	B	C
7.3				
Пункт(ы) прохода посетителей в офисной зоне				
7.3.1	Пункты прохода посетителей в офисную зону контролируются ответственным лицом/сотрудником охраны/работником ресепшн, прошедшим обучение по процедуре приема посетителей, выдаче пропусков, ведения журнала учёта посетителей и требованиям по наличию сопровождающего (в т.ч. процедура по допуску посетителей в нерабочее время).	✔	✔	✔
7.3.2	Пункты прохода посетителей просматриваются системой видеонаблюдения (цветными камерами или камерами, работающими в режиме «день/ночь»), физические лица должны быть четко различимы в любой момент.	✔	✔	

Раздел	Входные группы офиса и склада	A	B	C
7.3.3	Кнопка тревожной сигнализации установлена в скрытом месте на стойке ресепшн в зоне приема посетителей и тестируется на еженедельной основе.	✔	✔	
7.3.4	Идентификация личности посетителей осуществляется по документам, выданным государственными органами, имеющим фотоизображение владельца (например, водительское удостоверение, паспорт, национальное ID и т. д.).	✔	✔	✔
7.3.5	Все посетители регистрируются в журнале учёта посетителей, записи в котором хранятся минимум 30 дней.	✔	✔	✔
7.3.6	Временные пропуска посетителей сдаются при завершении визита на объект; записи в журнале учета посетителей сверяются на ежедневной основе.	✔	✔	
7.3.7	При нахождении на территории объекта все посетители обязаны иметь временные пропуска, размещенные на видном месте поверх одежды и постоянно сопровождаются сотрудником компании.	✔	✔	
Пункт(ы) прохода персонала				
7.3.8	Пункты пропуска персонала на объект контролируются круглосуточно (24/7).		✔	✔
7.3.9	Пункты прохода персонала контролируются с помощью СКУД в режиме 24/7. Данные о проходе сотрудников фиксируются электронным способом.	✔		
7.3.10	Пункты прохода персонала находятся под видеонаблюдением (цветные или работающие в режиме «день/ночь» камеры).	✔	✔	
7.3.11	При трудоустройстве, после прохождения проверочных процедур, всем штатным сотрудникам выдаются постоянные пропуска/ID-карты, имеющие фотоизображение владельца.	✔	✔	
7.3.12	Всему остальному персоналу выдаются пропуска/ID-карты, позволяющие идентифицировать их во время нахождения на объекте.	✔	✔	
7.3.13	Все сотрудники размещают пропуска/ID-карты на видном месте поверх одежды.	✔	✔	
7.3.14	Пропуска сотрудников ни при каких обстоятельствах не могут быть переданы другим лицам. На объекте должна быть внедрена политика по обращению с пропусками.	✔	✔	
Идентификация водителей и транспортных средств				
7.3.15	Все водители проходят процедуру идентификации с использованием удостоверений личности, выданных государственными органами и имеющими фотоизображение владельца (например, водительское удостоверение, паспорт, национальная ID карта и т. д), ведётся журнал учёта водителей.	✔	✔	✔
7.3.16	Производится проверка подлинности документов, удостоверяющих личность водителей, водительских удостоверений и их сроков их действия.	✔	✔	✔

Раздел	Входные группы офиса и склада	A	B	C
7.3.17	Идентификационные данные транспортных средств заносятся в журнал учёта вручную или с помощью камер видеонаблюдения и включают, как минимум, государственный регистрационных знак и тип ТС.	✔		

Раздел	Внутреннее пространство склада и офиса	A	B	C
7.4				
Разграничение зон хранения ТМЦ разных клиентов				
7.4.1	Внутренние стены и крыша здания, разделяющие зоны хранения товаров разных клиентов, спроектированы/сконструированы таким образом и поддерживаются в надлежащем состоянии, чтобы воспрепятствовать несанкционированному проникновению (например: из кирпича, блоков, сборных бетонных плит, сэндвич-панелей).	✔	✔	✔
7.4.2	Если внутренние перегородки между зонами хранения разных клиентов сконструированы из высокопрочной защитной сетки или иного защитного материала, отвечающего требованиям безопасности в отрасли, физическое ограждение также должно быть оборудовано охранной сигнализацией для обнаружения проникновения. *Примечание: запрещается использовать бытовую сетку (сетка-рабица) и другие низкокачественные виды ограждения, не обеспечивающие защитных свойств.*	✔	✔	✔
Внутреннее пространство склада				
7.4.3	Система охранной сигнализации (например, инфракрасные датчики, датчики движения, звука или вибро-датчики) должна быть установлены для контроля внутреннего пространства склада. В нерабочее время (например, когда склад закрыт) внутренняя зона склада должна быть поставлена на сигнализацию, а сигналы с датчиков выведены на основной пульт охраны. *Примечание: если склад работает в режиме 24/7/366, данное требование может быть неприменимо в случае, когда риски и меры по их снижению документально отражены в ежегодной оценке рисков.* *Независимо от режима работы объекта, датчики охранной сигнализации, установленные по периметру, или физические ограждение должны присутствовать на внешних дверях и окнах, расположенных на уровне земли, в офисе и на складе (см. раздел 7.2.11).*	✔		
Внутренняя зона ворот грузовых доков				
7.4.4	Вся внутренняя зона грузовых доков покрыта камерами системы видеонаблюдения (цветные или работающие в режиме «день/ночь»).	✔	✔	✔
7.4.5	Обзор камерами видеонаблюдения погрузочно-разгрузочных работ во внутренней зоне доков никогда не перекрывается за исключением кратковременных промежутков, вызванных производственной необходимостью (например, текущая загрузка и разгрузка транспортного средства).	✔	✔	✔

Раздел	Внутреннее пространство склада и офиса	A	B	C
7.4.6	Движение товарно-материальных ценностей Заказчика в зонах хранения и комплектации (т.е. в зонах разборки/формирования паллет, на маршрутах от/до стеллажей, у грузовых доков, в транзитных коридорах) на 100% покрыто системой видеонаблюдения.	✔	✔	
Контроль доступа между офисом и складом				
7.4.7	Доступ из офисной части объекта в зону хранения находится под контролем.	✔	✔	
7.4.8	Считыватели СКУД или домофоны на дверях между офисом и складской зоной оборудованы звуковой сигнализацией. В случае если дверь остается открытой дольше 60 секунд, активируется локальный звуковой сигнал тревоги. В случае несанкционированного вскрытия двери звуковой сигнал подаётся незамедлительно.	✔		
7.4.9	Двери между офисной и складской зонами оборудованы сигнализацией, которая издает звуковой сигнал **или** посылает сигнал тревоги на пульт охраны, требующий реагирования, если двери остаются открытыми на протяжении 60 сек. или подверглись несанкционированному вскрытию.		✔	
7.4.10	Штатные сотрудники ПЛУ/Заявителя и сопровождаемые ими посетители имеют доступ во внутреннюю складскую зону/зону доков, исходя из ограничений согласно их служебным обязанностям.	✔	✔	✔
7.4.11	Список лиц, допущенных в зону хранения и доков, пересматривается как минимум раз в квартал с целью ограничить излишние права доступа и убедиться, что доступ предоставляется только уполномоченному персоналу.	✔	✔	
Закрытые зоны хранения товаров повышенной категории риска (ЗЗХ)				
7.4.12	Размер и назначение закрытых зон хранения (ЗЗХ) может быть определен в договоре между Заказчиком и ПЛУ/Заявителем. При отсутствии требований, прописанных в договоре, ЗЗХ должна обеспечивать хранение товаров в объеме не менее 6 куб. метров.	✔	✔	
7.4.13	Периметр ЗЗХ огорожен решеткой или имеет усиленное ограждение со всех сторон, включая верх/крышу.	✔	✔	
7.4.14	Запирающее устройство установлено на дверях/воротах ЗЗХ.	✔	✔	
7.4.15	Камеры видеонаблюдения (цветные или работающие в режиме «день/ночь») полностью просматривают вход в ЗЗХ и её внутреннее пространство. *Примечание: если размер ЗЗХ не позволяет разместить камеру видеонаблюдения внутри, допускается наличие видеонаблюдения только за входом.*	✔		
7.4.16	Камеры видеонаблюдения (цветные или работающие в режиме «день/ночь») просматривают вход в ЗЗХ.		✔	

Раздел	Внутреннее пространство склада и офиса	A	B	C
7.4.17	Если допуск в ЗЗХ имеют 10 и более сотрудников объекта, доступ должен контролироваться электронным способом (карта СКУД/электронный брелок). Если доступ требуется менее чем для 10 сотрудников, допускается использование механических запорных устройств (навесной замок и т.п.) при наличии процедуры учёта и контроля выдачи ключей. Ключи могут быть выданы сотруднику на время смены, но их нельзя предавать без разрешения и соответствующих записей в журнале учёта выдачи ключей. Все ключи должны быть возвращены на место и учтены, когда они не используются.	✔		
7.4.18	Двери/ворота ЗЗХ оборудованы датчиками охранной сигнализации для обнаружения несанкционированного проникновения. Сигналы тревоги могут генерироваться контактными датчиками, установленными на дверях, и/или инициироваться датчиком движения системы видеонаблюдения.	✔		
7.4.19	Ограждение ЗЗХ поддерживается в исправном состоянии и ежемесячно инспектируется на предмет целостности и наличия повреждений.	✔		
7.4.20	ПЛУ/Заявитель обязан обеспечить соблюдение того, что доступ в ЗЗХ предоставлен исключительно уполномоченному персоналу. Список лиц, имеющих доступ к ЗЗХ, пересматривается ежемесячно и обновляется незамедлительно, если уполномоченный сотрудник увольняется или больше не нуждается в доступе. Предоставление доступа в ЗЗХ регулируется соответствующей процедурой.	✔	✔	
Контроль за сбором и вывозом мусора				
7.4.21	Все основные места сбора мусора, зоны консолидации отходов (пресс-компакторы) внутри и снаружи склада, контролируются с помощью системы видеонаблюдения.	✔		
7.4.22	Где применимо, мешки для сбора мусора в зоне хранения выполнены из прозрачного материала.		✔	✔
Подготовка ТМЦ и предварительная загрузка ТС				
7.4.23	Не допускается предварительная погрузка и размещение транспортных средств с грузом Заказчика в нерабочие часы снаружи складского помещения, если иное не оговорено между Заказчиком и ПЛУ/Заявителем. Альтернативные меры безопасности должны быть предусмотрены на случай, если предварительная отгрузка ТС согласована (например, дополнительные устройства безопасности на контейнере). *Примечание: «снаружи складского помещения» означает, что эти зоны отделены от здания склада, но находятся на территории ПЛУ/Заявителя внутри ограждения по периметру.*	✔	✔	✔
Пронос личных вещей и осмотр персонала				
7.4.24	Утвержденная письменная процедура определяет порядок контроля за проносом личных вещей (персональных контейнеров) сотрудниками внутрь склада. К персональным контейнерам относятся ланчбоксы, рюкзаки, сумки, кошельки и т. д.	✔	✔	

Раздел	Внутреннее пространство склада и офиса	A	B	C
7.4.25	Если это предусмотрено местным законодательством, на объекте должна быть разработана и внедрена процедура осмотра сотрудников при выходе с объекта. Критерии для проведения осмотра сотрудника определяются ПЛУ/Заявителем и/или закреплены условиями договора Заказчика и ПЛУ/Заявителя. Как минимум, процедура должна предусматривать возможность проведение осмотра, если возникает необходимость в случае, когда этого обычно не требуется (например, при подозрении сотрудника в совершении кражи).	✔		
Контроль погрузочно-разгрузочной техники				
7.4.26	Процедура предусматривает, что вся погрузочно-разгрузочная техника с электрическим приводом внутри склада отключена и обесточена в нерабочее время. *Примечание: исключение составляют гидравлические ручные погрузчики/тележки для перевозки паллет/поддонов.*	✔	✔	
Целостность контейнеров и прицепов «7-point inspection»				
7.4.27	Физическая инспекция целостности периметра грузовых отсеков транспортных средств (7-point physical inspection) проводится перед отгрузкой контейнеров или прицепов, следующих в адрес Заказчика. Проверка включает осмотр всех бортов, передней стенки, пола, крыши, ворот и запирающих механизмов, наружной части днища платформы и шасси. *Примечание: данное требование относится ко всем типам прицепов и контейнеров, которые запираются/опломбируются (а не только к контейнерам для морских перевозок).*	✔	✔	✔
Процесс приёма-передачи груза: Пломбировочные устройства				
7.4.28	Если иное не согласовано с Заказчиком, все грузовые транспортные средства, следующие в прямом, безостановочном сообщении, должны быть опломбированы пломбами повышенной защищенности, сохраняющими признаки несанкционированного вскрытия. Пломбировочные устройства должны соответствовать стандарту ISO 17712 (классификация I, S или H). *Примечание: опломбирование ТС не требуется, если на маршруте запланировано несколько пунктов выгрузки из-за сложности и риска того, что водитель должен иметь при себе несколько пломб.*	✔	✔	✔
7.4.29	ПЛУ/Заявитель должен иметь документально утвержденные процедуры контроля и учёта пломбировочных устройств, состояния запорных устройств прицепа (контейнера), штифтовых замков и прочего оборудования безопасности.	✔	✔	✔
7.4.30	Пломбировочные устройства могут навешиваться или сниматься только уполномоченным персоналом, то есть сотрудниками склада, прошедшими инструктаж по выявлению признаков несанкционированного вскрытия и повторного навешивания пломб. Водителям запрещается самостоятельно опломбировать грузовой отсек или снимать пломбу, за исключением случаев, когда такое право предоставлено Заказчиком.	✔	✔	✔

Раздел	Внутреннее пространство склада и офиса	A	B	C
7.4.31	Внедрена процедура по выявлению скомпрометированных пломб, подвергшихся несанкционированному вскрытию и повторному навешиванию в пути следования.	✔	✔	✔
Целостность груза. Проверка соответствия при погрузке/разгрузке				
7.4.32	Внедрены процедуры, обеспечивающие проведение проверки соответствия всех исходящих и входящих потоков ТМЦ Заказчика путем поштучного пересчёта мест вручную и/или с помощью электронных средств. Процесс должен обеспечить выявление несоответствий, которые отражаются в отчётах ПЛУ/Заявителю и/или Заказчику. Записи и/или электронные отчеты должны быть выполнены в формате, предоставляющем доказательную основу. Если водители не присутствуют при отгрузке товара, Заказчик/ПЛУ/Заявитель должен представить иные свидетельства о количестве отгруженного товара, например, записи и/или изображения с камер видеонаблюдения, собранные и хранящиеся специально для этой цели. *Примечание: помимо непосредственно недостающего товара, несоответствия могут включать повреждения упаковки, отсутствие упаковочной ленты, порезы или иные хорошо различимые отверстия, что указывает на вероятность совершения кражи.*	✔	✔	✔
Предотвращение получения груза по поддельным документам				
7.4.33	Для предотвращения риска мошенничества и выдачи груза по поддельным документам, перед отгрузкой сотрудники склада-отправителя обязаны проверить документы, удостоверяющие личность водителя, документы, подтверждающие его право получения груза и сравнить их с данными предварительного уведомления, полученного от Заказчика. Внедрена соответствующая процедура.	✔	✔	✔

Section	Системы безопасности: предназначение, мониторинг и реагирование	A	B	C
7.5				
Пульт охраны и мониторинга				
7.5.1	Мониторинг сигналов тревоги осуществляется в круглосуточном режиме (24x7x366) посредством собственного или внешнего пульта охраны и мониторинга, помещение которого защищено от несанкционированного доступа. *Примечание: пульт охраны и мониторинга может располагаться как на территории объекта, так и за его пределами, и может принадлежать как самой компании ПЛУ, так и третьей стороне. Во всех случаях доступ в помещение мониторинга должен контролироваться с помощью системы контроля доступа (электронные карты), замков или биометрических сканеров.*	✔	✔	✔
7.5.2	Реагирование на все сигналы тревоги от систем безопасности происходит в режиме реального времени 24x7x366.	✔	✔	✔
7.5.3	Пульт охраны подтверждает поступление сигнала тревоги и инициирует процедуру эскалации в течение 3 минут с момента его получения.	✔	✔	✔

Section	Системы безопасности: предназначение, мониторинг и реагирование	A	B	C
7.5.4	Отчеты о срабатывании систем безопасности имеются наличии и доступны для проверки.	✔	✔	✔
7.5.5	Процедуры реагирования на сигналы тревоги пульта охраны и мониторинга закреплены документально.	✔	✔	✔
Система охранной сигнализации				
7.5.6	Система охранной сигнализации активируется в нерабочее время, а сигналы выводятся на центральный пульт охраны.	✔	✔	✔
7.5.7	Отчеты о срабатывании системы охранной сигнализации сохраняются в течение 60 дней.	✔	✔	
7.5.8	Отчеты о срабатывании системы охранной сигнализации хранятся в защищенном месте, производится их регулярное резервное копирование.	✔		
7.5.9	Отчеты о срабатывании системы охранной сигнализации хранятся в защищенном месте.		✔	
7.5.10	Утверждена процедура, определяющая права доступа к системе охранной сигнализации для уполномоченных сотрудников и системных администраторов. Это касается доступа к серверам, консолям, контроллерам, панелям, сетям и данным. Права доступа в систему должны незамедлительно обновляться после того, как лица, имеющие доступ, увольняются из компании или переходят на должность, не связанную с работой в системе.	✔	✔	✔
7.5.11	Система охранной сигнализации посылает сигнал тревоги в случае перебоев/отключения её питания. *Примечание: в системах, где используются источники бесперебойного питания (ИБП), сигнал тревоги передаётся в случае неисправности работе батареи ИБП.*	✔	✔	✔
7.5.12	Внедрена процедура проверки постановки системы на сигнализацию. *Примечание: документально закрепленная процедура проверки того, что объект поставлен на сигнализацию в нерабочее время.*	✔	✔	✔
7.5.13	Система охранной сигнализации посылает сигнал тревоги по основному каналу в случае сбоев в работе датчиков сигнализации и/или шлейфов.	✔	✔	
7.5.14	Система охранной сигнализации имеет резервный канал передачи сигналов на случай сбоев в работе датчиков и/или шлейфов.	✔	✔	
Система контроля управления доступом (СКУД)				
7.5.15	Отчёты о событиях в СКУД хранятся в течение 90 дней. Отчёты хранятся в защищенном месте; производится их регулярное резервное копирование.	✔	✔	

Section	Системы безопасности: предназначение, мониторинг и реагирование	A	B	C
7.5.16	Утверждена процедура, определяющая права доступа к системе управления контролем доступа для уполномоченных сотрудников и системных администраторов. Права доступа в систему должны незамедлительно обновляться после того, как лица, имеющие доступ, увольняются из компании или переходят на должность, не требующую доступа в СКУД.	✔	✔	
7.5.17	Обзор отчётов о работе СКУД производится как минимум раз в квартал в целях выявления нарушений в работе системы или её нецелевого использования (например, неоднократных безуспешных попыток доступа, ошибочного считывания заблокированной карты, свидетельства передачи карты третьим лицам для несанкционированного доступа и т. д.). Процесс документально закреплен.	✔	✔	
Система видеонаблюдения				
7.5.18	Запись в системе видеонаблюдения осуществляется в цифровом формате.	✔	✔	✔
7.5.19	Скорость записи в системе видеонаблюдения установлена на уровне не менее 8 кадров с секунду на камеру. *Примечание: TAPA разрешает обладателям текущих сертификатов, не имеющих технических возможностей увеличить скорость до 8 кадров в секунду, продолжить использование оборудования, работающего на скорости 3 кадра в сек. до вступления в силу версии РБО 2023 г. Все новые ПЛУ/Заявители должны соответствовать вышеуказанным требованиям.*	✔	✔	✔
7.5.20	Работоспособность системы видеонаблюдения проверяется ежедневно в рабочие дни на основе документально закрепленной процедуры. Записи имеются в наличии.	✔	✔	✔
7.5.21	Записи с камер видеонаблюдения должны храниться как минимум 30 дней, если это не противоречит местному законодательству. В противном случае ПЛУ/Заявитель обязан предоставить доказательство того, что видеонаблюдение запрещено законодательно и/или разрешенный срок хранения записей системы составляет менее 30 дней.	✔	✔	✔
7.5.22	Доступ к системе видеонаблюдения, включая оборудование, программное обеспечение и хранение данных/видеоматериалов, строго контролируется.	✔	✔	✔
7.5.23	Изображения камер системы видеонаблюдения в целях безопасности разрешается просматривать только уполномоченному персоналу.	✔	✔	✔
7.5.24	Утверждена письменная процедура, подробно описывающая политику защиты данных системы видеонаблюдения, её текущих и архивных изображений на соответствие местному законодательству.	✔	✔	
Внешнее и внутреннее освещение				
7.5.25	На объекте поддерживается достаточный уровень внешнего и внутреннего освещения для обеспечения чёткости изображений камер системы видеонаблюдения при использовании в ходе расследований и получения записей изображений необходимого качества.	✔	✔	

Section	Системы безопасности: предназначение, мониторинг и реагирование	A	B	C
7.5.26	Внешнее и внутреннее освещение достаточно для идентификации всех транспортных средств и физических лиц.	✔		

Раздел	Обучение и Процедуры	A	B	C
7.6				
Процедуры эскалации				
7.6.1	Утвержденные, постоянно действующие письменные процедуры по обращению с товарно-материальными ценностями Заказчика включают его своевременное уведомление об утрате, недостаче или хищении имущества. О любых инцидентах ПЛУ/Заявитель обязан проинформировать Заказчика в течение 24 часов. О явных фактах хищений сообщается незамедлительно. Обеспечивается последовательное соблюдение данных требований.	✔	✔	✔
7.6.2	Контактная информация в виде списков представителей Заказчика и руководства объекта ПЛУ/Заявителя на случай чрезвычайных ситуаций имеется в наличии. Списки обновляются каждые 6 месяцев и включают контакты дежурных служб правоохранительных органов.	✔	✔	✔
Приверженность руководства поддержанию РБО				
7.6.3	Руководство объекта должно официально назначить лицо, ответственное за обеспечения безопасности на объекте, которое также отвечает за поддержание требований РБО TAPA и безопасность цепи поставок предприятия. Поставщик должен также назначить сотрудника (это может быть одно и то же лицо) для контроля соответствия программе РБО. В обязанности данных сотрудников должно входить планирование проверок выполнения требований, поддержку связи с УА, последующую сертификацию, отслеживание изменений в стандарте РБО и пр. *Примечание: указанные лица могут быть штатными сотрудниками или отдельно нанятыми работниками в рамках контракта на исполнение данной функции.*	✔	✔	✔
7.6.4	Руководство должно разработать, довести до сведения персонала и поддерживать документально закрепленную политику по безопасности для обеспечения того, что все соответствующие лица (штатные сотрудники и подрядчики) должным образом осведомлены о требованиях компании в области безопасности.	✔	✔	✔

Раздел	Обучение и Процедуры	A	B	C
7.6.5	Оценка рисков на объекте по определению вероятности и последствий инцидентов, связанных с нарушением безопасности, должна проводиться/обновляться как минимум ежегодно. Процесс оценки рисков должен быть документально закреплен и отражать обязанности руководства по принятию компетентных решений по снижению уязвимостей и минимизации рисков. Необходимо проанализировать как минимум следующие общие типы внутренних/внешних угроз: кража груза или информации, несанкционированное проникновение на объект или доступ к ТМЦ, повреждение/уничтожение систем безопасности, отгрузка по поддельным документам, обеспечение непрерывности деятельности и поддержания безопасности на объекте в условиях нехватки штатного персонала или стихийных бедствий и пр. С учетом локальных/страновых особенностей и рисков могут рассматриваться другие события и виды угроз.	✔	✔	✔
Обучение				
7.6.6	Обучение по требованиям безопасности и существующим угрозам для всего штатного персонала проводится в течение первых 60 дней после принятия сотрудников на работу и в дальнейшем каждые 2 года.	✔	✔	✔
7.6.7	Обучение по информационной безопасности штатных сотрудников, имеющих доступ к информации Заказчика, направленно на защиту данных о движении материальных ценностей Заказчика, хранящихся в электронном виде и на бумажных носителях.	✔	✔	
Доступ к имуществу Заказчика				
7.6.8	На объекте имеются документально закрепленные процедуры по защите имущества Заказчика от несанкционированного доступа со стороны штатных сотрудников, посетителей и пр.	✔	✔	
Контроль доступа к информации				
7.6.9	Доступ к товаросопроводительной документации и информации об имуществе Заказчика предоставляется исходя из принципа «служебной необходимости».	✔	✔	✔
7.6.10	Доступ к товаросопроводительной документации и информации Заказчика контролируется и ведется его учёт.	✔	✔	✔
7.6.11	Товаросопроводительная документация и информация Заказчика хранится в защищенном месте до момента планового уничтожения.	✔	✔	✔
Система учёта инцидентов безопасности				
7.6.12	На объекте внедрена система учёта и анализа инцидентов безопасности, которая используется для определения превентивных мер.	✔	✔	
Программа технического обслуживания				

Раздел	Обучение и Процедуры	A	B	C
7.6.13	Документально закрепленные регламенты технического обслуживания всех технических (физических) систем безопасности (например, система видеонаблюдения, СКУД, системы охранной сигнализации и освещения) имеются в наличии в целях обеспечения их непрерывной работы.	✔	✔	✔
7.6.14	Профилактическое техническое обслуживание проводится раз в год или в соответствии с требованиями производителя оборудования.	✔	✔	✔
7.6.15	Проверка работоспособности всех систем безопасности проводится раз в неделю и регистрируется документально, за исключением случаев, когда сигнал о неисправности фиксируется самой системой незамедлительно/ автоматически.	✔	✔	
7.6.16	Выполнение заявки на устранение неисправностей должно быть начато в течение 48 часов или непосредственно в момент обнаружения неисправности. Для любых ремонтных работ, срок проведения которых превышает 24 часа, должны быть приняты альтернативные меры по снижению рисков.	✔	✔	
Инструктаж подрядчиков				
7.6.17	ПЛУ/Заявитель должен обеспечить проведение инструктажа и обеспечить соблюдение всеми сотрудниками подрядных организаций и поставщиков по существующим мерам безопасности на объекте ПЛУ/Заявителя.	✔	✔	✔
Записи системы учёта ТМЦ				
7.6.18	Товаросопроводительная документация должна отвечать требованиям местного законодательства, быть разборчиво и полностью заполнена (с указанием времени, даты, подписей, данных о водителе, сотрудниках, участвовавших в погрузке/разгрузке, с подробной информацией о транспортном средстве, количестве товара и т. д.).	✔	✔	✔
7.6.19	ПЛУ/Заявитель должен сохранять записи о всех отгруженных ТМЦ и доставленных грузах в течение как минимум двух лет и, при необходимости, обеспечить к ним доступ при расследовании инцидентов.	✔	✔	✔
7.6.20	Подтверждение доставки осуществляется в соответствии с требованиями, прописанными в договоре между Заказчиком и ПЛУ/Заявителем. Если предусмотрено требованиями Заказчика, грузополучатель обязан уведомлять отправителя в оговоренный срок о получении груза согласно сведениям, указанным в предварительном уведомлении об отправке.	✔	✔	✔
Процедура предварительного уведомления				

Раздел	Обучение и Процедуры	A	B	C
7.6.21	По требованию Заказчика, в отношение входящих/исходящих грузовых потоков может применяться процедура предварительного уведомления об отправке. Форма и содержание предварительного уведомления должны быть согласованы между Заказчиком и ПЛУ/Заявителем. В форму предварительного уведомления рекомендовано включение следующих деталей: время отправления, ожидаемое время прибытия, название транспортной компании, имя водителя, государственный регистрационный знак ТС, информация о грузе (количество грузовых мест, вес, номер транспортной накладной и т. д.) и номера пломб(ы) грузового отсека.	✔	✔	✔

Раздел	Процедуры безопасности в отношение персонала	A	B	C
7.7				
7.1	Отбор, изучение и проверка персонала (при условии соответствия требованиям местного законодательства)			
7.7.1	ПЛУ/Заявитель должен иметь процедуры отбора, изучения и проверки персонала, включающие, как минимум, сведения о предыдущих местах работы и информацию об наличии судимости. Данное требование применяется ко всем кандидатам, включая сотрудников и подрядчиков, а также к аутсорсинговым компаниям, предоставляющими временный агентский персонал (TAS).	✔	✔	✔
7.7.2	Сотрудники из числа временного агентского персонала должны подписывать декларацию об отсутствии у них текущей судимости и своём согласии следовать требованиям и процедурам безопасности ПЛУ/Заявителя.	✔	✔	✔
7.7.3	Договоры с агентствами по найму персонала предусматривают передачу ПЛУ/Заявителю информации проведении процедур отбора, изучения и проверки в отношение временного агентского персонала. В противном случае ПЛУ/Заявитель должен проводить данные проверки самостоятельно. Процедура должна предусматривать проверку на судимость и отзывы с предыдущих мест работы.	✔	✔	✔
7.7.4	Внедрена процедура по действиям в случае предоставления кандидатами/штатными сотрудниками недостоверной информации как до, так и после приема на работу.	✔	✔	✔
Увольнение сотрудников или повторный найм *Примечание: прекращение трудовых отношений подразумевает под собой как вариант увольнения по соглашению сторон, так и принудительные увольнения сотрудников*				
7.7.5	При увольнении сотрудники должны вернуть свои служебные удостоверения, карты доступа, ключи, оборудование и носители информации. Требуется наличие документальной процедуры.	✔	✔	✔

Раздел	Процедуры безопасности в отношение персонала	A	B	C
7.7.6	Защита данных Заказчика: при увольнении сотрудника ПЛУ/Заявитель обязан отключить доступ к любым системам, содержащим данные Заказчика (системы инвентарного учёта, графики отгрузок и т.д.). Требуется наличие документальной процедуры.	✔	✔	✔
7.7.7	Процедурами утверждена форма обходного листа.	✔	✔	✔
7.7.8	Повторный найм на работу: Имеются утвержденные процедуры для предотвращения повторного найма сотрудников ПЛУ/Заявителем при наличии действующих оснований для отказа в приёме на работу. *Примечание: перед повторным приемом на работу изучаются причины прекращения трудовых отношений (Например, обстоятельства предыдущего увольнения или отказа кандидату в трудоустройстве).*	✔	✔	✔

8. Функция Центрального управления (действует только для варианта одновременной сертификации нескольких объектов)

Раздел	Функция Центрального Управления	A	B	C
8.1	**Общие положения**			
8.1.1	Функция Центрального Управления предназначена для управления системой менеджмента безопасности для всех объектов, как определено в области применения при проведении одновременной сертификации нескольких объектов.	✔	✔	✔
8.1.2	Все объекты должны иметь юридические или договорные отношения с Функцией Центрального управления.	✔	✔	✔
8.1.3	Единая система менеджмента безопасности внедрена для обеспечения того, что все объекты в рамках системы отвечают требованиям используемого стандарта безопасности TAPA.	✔	✔	✔
8.1.4	Функция центрального управления и её система менеджмента подлежат прохождению внутренних аудитов, чтобы обеспечить постоянное соответствие стандартам TAPA.	✔	✔	✔
8.1.5	Функция центрального управления должна проводить собственные аудиты различных объектов, чтобы гарантировать соответствие системы менеджмента безопасности требованиям применяемых стандартов и её способность достичь целей безопасности для всех объектов ПЛУ/Заявителя. Аудиты проводятся с использованием утвержденных форм аудита TAPA.	✔	✔	✔
8.1.6	Функция центрального управления должна иметь необходимые права и полномочия для того, чтобы потребовать от всех объектов соблюдения требований стандарта TAPA и выполнения корректирующих и превентивных меры в случае необходимости. *Примечание: там, где применимо, это должно быть указано в официальном соглашении между функцией центрального управления и объектами.*	✔	✔	✔
8.2	**Политики и Процедуры**			
8.2.1	Функция центрального управления должна поддерживать документированные политики и процедуры для своей системы менеджмента безопасностью, которые применимы ко всем ее объектам.	✔	✔	✔
8.2.2	Функция центрального управления должна обеспечить, что все соответствующие политики и процедуры обновляются, доводятся до сведения, размещаются и внедряются на всех объектах по мере необходимости.	✔	✔	✔
8.2.3	Политика и процедуры должны поддерживаться и быть легко доступны для всех объектов по мере необходимости.	✔	✔	✔
8.3	**Внутренние аудиты объектов**			
8.3.1	Функция центрального управления должна поручить всем объектам проводить внутренние аудиты, все отчеты о которых должны быть направлены в функцию центрального управления для учёта и анализа.	✔	✔	✔
8.3.2	Функция центрального управления должна гарантировать, что все ТКМБ, зафиксированные по итогам внутренних аудитов, надлежащим образом выполнены в интересах улучшения ее систем менеджмента безопасностью.	✔	✔	✔

Раздел	Функция Центрального Управления	A	B	C
8.3.3	Все объекты должны предоставлять сведения о ходе реализации мер и отчеты по всем невыполненным ТКМБ в функцию центрального управления. Центральная функция должна уведомлять руководство ПЛУ/ Заявителя, в случае, если ТКМБ не завершены в установленные сроки.	✔	✔	✔
8.4	**Записи о проверках, журналы учёта и другие инспекции**			
8.4.1	Функция центрального управления должна внедрить процедуру, обеспечивающую поддержание всеми объектами записей о проведении проверок, ведении журналов учёта посетителей, водителей и проведении инспекций целостности грузового отсека транспортных средств '7-point inspection'.	✔	✔	✔
8.5	**Оценка рисков на всех объектах**			
8.5.1	Функция центрального управления должна иметь процедуры, обеспечивающие проведение надлежащей оценки рисков и управления ими на всех объектах системы, а также ведение соответствующих записей.	✔	✔	✔
8.6	**Документация систем видеонаблюдения и охранной сигнализации**			
8.6.1	Функция центрального управления должна иметь процедуры, которые гарантируют, что все объекты проверяют и поддерживать документацию по всем системам физической безопасности, таким как видеонаблюдение и охранная сигнализация.	✔	✔	✔
8.7	**Поддержание системы охранной сигнализации и СКУД**			
8.7.1	Функция центрального управления должна иметь процедуры, обеспечивающие обслуживание и тестирование всех систем охранной сигнализации и контроля доступа для обеспечения их операционной эффективности.	✔	✔	✔
8.7.2	Функция центрального управления должна иметь процедуры, обеспечивающие ведение записей на всех объектах обо всех инцидентах и тестах систем охранной сигнализации и контроля доступа.	✔	✔	✔
8.8	**Учёт обучения персонала**			
8.8.1	Функция центрального управления внедряет процедуры для обеспечения того, чтобы на всех объектах велись надлежащие записи о прохождении сотрудниками обучения в области менеджмента безопасности.	✔	✔	✔
8.8.2	Функция центрального управления внедряет процедуры для обеспечения того, чтобы на всех объектах велись записи о прохождении персоналом объекта обучения в области противодействия угрозам безопасности.	✔	✔	✔
8.9	**Записи об изучении и проверке кандидатов**			
8.9.1	Функция центрального управления должна иметь процедуры, гарантирующие, что все объекты регулярно проводят проверку и изучение кандидатов перед приёмом на работу, чтобы гарантировать целостность и эффективность систем управления безопасностью.	✔	✔	✔

Раздел	Функция Центрального Управления	A	B	C
8.9.2	Функция центрального управления должна иметь процедуры, обеспечивающие ведение записей с анализом, включая выводы и корректирующие/предупреждающие меры указанные в п. 8.1.6.	✔	✔	✔
8.10	**Анализ и оценка руководством системы менеджмента безопасности**			
8.10.1	Функция центрального управления должна проводить регулярный анализ и обзор всех процессов для обеспечения соответствия, эффективности и постоянного улучшения системы менеджмента безопасности.	✔	✔	✔
8.10.2	Анализ со стороны руководства должен, среди прочего, охватывать эффективность программы внутренних аудитов, выполнения ТКМБ, проведения оценки рисков, управления инцидентами и меры по улучшению.	✔	✔	✔
8.10.3	Функция центрального управления должна вести учёт записей о проведении анализа и обзоров.	✔	✔	✔

9.0. Угрозы ИТ- и кибербезопасности – Дополнительные опции

РБО включает дополнительные меры по защите от киберугроз, которые предоставляют более высокий уровень защиты и могут использоваться в дополнение к основным разделам стандарта. Эта дополнительная опция обеспечивает возможность выбора ПЛУ/Заявителем и/или их Заказчиком в качестве дополнительных требований для обеспечения их операционных потребностей в безопасности. Когда дополнительная опция выбрана в ходе определения охвата программы РБО как часть сертификационного аудита, все её требования становятся обязательными.

Раздел	Угрозы ИТ и кибер-безопасности - Дополнительные опции
9.	***Обязательные требования***
9.1	У ПЛУ/Заявителя должны быть политики по ИТ и кибер-безопасности. Они могут быть оформлены одним или несколькими документами и должны охватывать следующие области: 1. Действия ПЛУ/Заявителя по идентификации и реагированию на угрозы. 2. Внедренные политики и процедуры по защите, выявлению, тестированию и реагированию на инциденты. 3. Методы восстановления ИТ-систем и/или данных. 4. Протоколы уведомления Заказчиков/Клиентов для снижения воздействия на цепи поставок в течение 24 часов с момента обнаружения инцидента. 5. Процедуры ежегодного пересмотра и обновления политик при необходимости.
9.2	ПЛУ/Заявитель должен поддерживать программу обучения для персонала по информационной безопасности. Она включает в себя: 1. Роль и ответственность пользователей компьютеров в поддержании безопасности и связанных с этим преимуществ. 2. Внедрена система учёта прохождении обучения персоналом, срок хранения записей в которой составляет не менее 2 лет.
9.3	ПЛУ/Заявитель должен внедрить документированную политику обеспечения мер кибер-безопасности у субподрядчиков и/или поставщиков, которая предусматривает следующее: 1. Требования ПЛУ/Заявителя по кибер-безопасности доведены до субподрядчика и/или поставщика и включены в договор. 2. При несогласии субподрядчика и/или поставщика следовать требованиям по кибер-безопасности ПЛУ/Заявителя, необходимо задокументировать и внедрить меры по снижению рисков ПЛУ/Заявителя и его клиентов.
9.4	ПЛУ/Заявитель должен внедрить план по предотвращению перебоев в электроснабжении, который обеспечивает питание критически важных ИТ-систем в течение не менее 48 часов, например, источник бесперебойного питания или резервный генератор.
9.5	Информационные системы ПЛУ/Заявителя должны быть защищены лицензированным антивирусным и антивредоносным программным обеспечением (ПО). Антивирусное и антивредоносное ПО должно иметь последние обновления.
9.6	ПЛУ/Заявитель должен иметь соответствующий план аварийного восстановления ИТ систем после атак со взломом системы, включая, помимо прочего, процедуру резервного копирования и восстановления всех необходимых данных и программного обеспечения

Раздел	Угрозы ИТ и кибер-безопасности - Дополнительные опции
9.7	Информационные системы ПЛУ/Заявителя должны проходить процедуру резервного копирования. Резервные копии системы должны регулярно тестироваться, а данные резервных копий должны быть зашифрованы и переданы на хранение за пределами головного офиса.
9.8	В целях управления и контроля доступа ПЛУ/Заявитель должен внедрить политику использования персональных идентификаторов и сложных паролей для доступа к информации со всех учетных записей. Данные процедуры должны обеспечивать: 1. Внедрена программа проверки паролей на соответствие политике. 2. При создании новой учетной записи должен назначаться уникальный пароль. 3. Первоначальные пароли не могут содержать имя пользователя, идентификационный номер или составляться по аналогии с пользовательскими данными. 4. Пароль доводится до сведения пользователя безопасным способом и только после его идентификации. 5. Пользователи обязаны сменить первоначальный пароль при первом входе в систему. 6. Пароли необходимо менять не реже одного раза в 90 дней.

Информация об издании и авторских правах

История публикаций

Впервые опубликовано в январе 2020

Впервые опубликовано (представлено) в январе 2020

Настоящая общедоступная спецификация вступает в силу1-го июля 2020.