

Оценка качества модели:		0.1961	0.2614	0.2512	BLEU score	Все три метрики показали, что наилучшие ответы дала модель с self-asking до основного вопроса, на втором месте модель с self-asking после основного вопроса
		0.7567	0.8217	0.8097	BERT Transformer	
		0.0125	0.1122	0.105	BERT Transformer	
	Вопрос	Ответ модели без self-asking	Ответ модели с self-asking до основного вопроса	Ответ модели с self-asking после основного вопроса	Правильный ответ	Документ для RAG
1	В составе ЗОКИИ имеется котельная, состоящая из ПЛК и АРМ. Каким образом необходимо выполнять требования приказа ФСТЭК России № 239, если установка наложенных СрЗИ невозможна?	<p>Если установка наложенных средств защиты информации (СрЗИ) невозможна на объекте критической информационной инфраструктуры (КИИ), то необходимо выполнить следующие действия:</p> <ol style="list-style-type: none"> 1. Определить базовый набор мер по обеспечению безопасности значимого объекта. 2. Выбрать меры по обеспечению безопасности значимых объектов для их реализации. 3. Разработать рабочую (эксплуатационную) документацию на значимый объект. 4. Описать архитектуру подсистемы безопасности значимого объекта. 5. Определить порядок и параметры настройки программных и программно-аппаратных средств, включая средства защиты информации. При этом следует учитывать, что выбор мер по обеспечению безопасности значимых объектов должен быть основан на категории значимости объекта КИИ и перечне нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект. 	<p>Для котельной, входящей в состав ЗОКИИ, могут быть использованы следующие меры по обеспечению безопасности:</p> <p>определение и обоснование организационных и технических мер, подлежащих реализации в рамках подсистемы безопасности значимого объекта;</p> <p>определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта;</p> <p>выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;</p> <p>разработка архитектуры подсистемы безопасности значимого объекта, включающей состав, места установки, взаимосвязи средств защиты информации;</p> <p>определение требований к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование угроз безопасности информации.</p>	<p>Если установка наложенных средств защиты информации (СрЗИ) невозможна на объекте критической информационной инфраструктуры (КИИ), то необходимо выполнить следующие действия:</p> <ol style="list-style-type: none"> 1. Определить базовый набор мер по обеспечению безопасности значимого объекта. 2. Выбрать меры по обеспечению безопасности значимых объектов для их реализации. 3. Разработать рабочую (эксплуатационную) документацию на значимый объект. 4. Описать архитектуру подсистемы безопасности значимого объекта. 5. Определить порядок и параметры настройки программных и программно-аппаратных средств, включая средства защиты информации. 6. Разработать правила эксплуатации программных и программно-аппаратных средств, включая средства защиты информации (правила безопасной эксплуатации). 7. Внедрить организационные и технические меры по обеспечению безопасности значимого объекта и ввести его в действие. При этом следует учитывать, что выбор мер по обеспечению безопасности значимых объектов должен быть основан на категории значимости объекта КИИ и перечне нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект. 	<p>Таким образом, для выполнения Требований к СБ в отношении автоматизированной системы управления котельной, состоящей из программируемых логических контроллеров и автоматизированных рабочих мест, необходимо:</p> <ol style="list-style-type: none"> 1. Определить базовый набор мер по обеспечению значимого объекта КИИ на основе его категории значимости. 2. Исключить из базового набора меры, которые не могут быть применены к объекту КИИ в соответствии с его техническими характеристиками. 3. Провести моделирование угроз безопасности информации. 4. Провести сопоставление угроз безопасности информации и мер, обеспечивающих блокирование данных угроз безопасности. 5. Разработать компенсирующие меры, обеспечивающие блокирование угроз безопасности информации или снижающие возможность их реализации, исходя из условий функционирования значимого объекта КИИ. 6. Провести приемочные испытания (аттестацию) значимого объекта КИИ и его подсистемы безопасности. 	Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) _Об утверждении Требований по обеспечен
2	Какие требования предъявляются к сотрудникам, ответственным за обеспечение безопасности ЗОКИИ и объектов без категории значимости (образование, должность, опыт работы и т.п.)?	<p>К работникам, ответственным за обеспечение безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ) и объектов без категории значимости, предъявляются следующие требования:</p> <ol style="list-style-type: none"> 1. Наличие высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению "Информационная безопасность". 2. Наличие стажа работы в сфере информационной безопасности не менее 3 лет. 	<p>Требования, предъявляемые к сотрудникам, ответственным за обеспечение безопасности ЗОКИИ и объектов без категории значимости, включают определение целей и задач обеспечения безопасности, основных угроз безопасности информации и категорий нарушителей, основных организационных и технических мероприятий по обеспечению безопасности, порядка применения, форм оценки соответствия значимых объектов критической информационной инфраструктуры и средств защиты информации требованиям по безопасности.</p>	<p>Дополнение ответа: К работникам, ответственным за обеспечение безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ) и объектов без категории значимости, предъявляются следующие требования:</p> <ol style="list-style-type: none"> 1. Наличие высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению "Информационная безопасность". 2. Наличие стажа работы в сфере информационной безопасности не менее 3 лет. 	<p>Согласно пункту 12 Требований к СОИБ, руководитель структурного подразделения по безопасности значимых объектов КИИ должен иметь высшее профессиональное образование в области информационной безопасности (далее – ИБ) либо иное высшее образование и прохождение профессиональной переподготовки по направлению «Информационная безопасность», а также иметь опыт работы в сфере ИБ не менее 3 лет.</p> <p>Сотрудники структурного подразделения по безопасности значимых объектов КИИ должны иметь высшее или среднее профессиональное образование по направлению «Информационная безопасность», либо высшее образование и повышение квалификации по аналогичному направлению. Требования к стажу данных сотрудников не предъявляются.</p> <p>И руководитель и сотрудники структурного подразделения по безопасности должны проходить повышение квалификации по профильному направлению не реже 1 раза в 3 года.</p> <p>Выполняемые данными сотрудниками обязанности по обеспечению безопасности значимых объектов КИИ должны быть определены в их должностных регламентах (инструкциях). Также Требования к СОИБ запрещают возложение на данных специалистов функций, не связанных с обеспечением безопасности значимых объектов КИИ или обеспечением ИБ субъекта КИИ в целом. Соответственно, такой специалист может выполнять только трудовые функции, направленные на обеспечение ИБ.</p>	Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) _Об утверждении Требований к созданию с
3	Какие организации допустимо привлекать для выполнения работ (оказания услуг) по ИБ в контексте подпункта «в» пункта 1 Указа Президента РФ № 250?	<p>Организации, имеющие в зависимости от информации, обрабатываемой значимым объектом критической информационной инфраструктуры, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации, могут быть привлечены для выполнения работ (оказания услуг) по информационной безопасности в контексте подпункта «в» пункта 1 Указа Президента РФ № 250.</p>	<p>Организации, имеющие лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на выполнение работ, связанных с использованием сведений, составляющих государственную тайну, и (или) на выполнение работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну, и (или) на проведение мероприятий и оказание услуг в области защиты государственной тайны.</p>	<p>В контексте подпункта «в» пункта 1 Указа Президента РФ № 250, организации, имеющие в зависимости от информации, обрабатываемой значимым объектом критической информационной инфраструктуры, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации, могут быть привлечены для выполнения работ (оказания услуг) по информационной безопасности.</p>	<p>Для выполнения мероприятий по обеспечению информационной безопасности (далее – ИБ) субъектов критической информационной инфраструктуры (далее – КИИ) по решению субъекта КИИ допустимо привлекать только организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации. Требования Указа Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» распространяются на всех субъектов КИИ.</p>	Указ Президента РФ от 01.05.2022 № 250 (ред. от 13.06.2024) _О дополнительных мерах по обеспечению и

4	Необходимо ли рассматривать силы иностранных государств в качестве нарушителей при моделировании угроз ЗОКИИ?	В контексте данного вопроса нет информации, которая бы указывала на необходимость рассмотрения сил иностранных государств в качестве нарушителей при моделировании угроз ЗОКИИ.	Да, при моделировании угроз безопасности значимых объектов критической информационной инфраструктуры необходимо учитывать силы иностранных государств как потенциальных нарушителей.	Нет необходимости рассматривать силы иностранных государств в качестве нарушителей при моделировании угроз ЗОКИИ.	Да, необходимо.	Методический документ. Методика оценки угроз безопасности информации. (утв. ФСТЭК России 05.02.2021)
5	В каком нормативном правовом акте установлены требования к безопасной разработке ПО – SCADA-систем?	Требования к безопасной разработке программного обеспечения (ПО) SCADA-систем установлены в следующих нормативных правовых актах: 1. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». 2. Постановление Правительства Российской Федерации от 3 февраля 2012 года № 79 «Об утверждении Правил разработки и утверждения федеральных целевых программ». 3. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	Требования к безопасной разработке программного обеспечения, включая SCADA-системы, установлены в Федеральном законе "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27 июля 2006 года.	Требования к безопасной разработке программного обеспечения (ПО) SCADA-систем установлены в следующих нормативных правовых актах: 1. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». 2. Постановление Правительства Российской Федерации от 3 февраля 2012 года № 79 «Об утверждении Правил разработки и утверждения федеральных целевых программ». 3. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	Требования по безопасной разработке программного обеспечения (далее – ПО) установлены в Требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ), утвержденных приказом ФСТЭК России от 25.12.2017 № 239 (далее – Требования к СБ). В соответствии с пунктом 29.3 Требования к СБ данные требования относятся ко всему прикладному ПО, которое обеспечивает выполнение функций значимого объекта КИИ в соответствии с его назначением. В том числе таким ПО являются SCADA-системы.	Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) _Об утверждении Требования по обеспечен
6	Возможны ли ситуации, когда объекты КИИ по определению из 187-ФЗ есть, но включать их в Перечень объектов КИИ нет необходимости, так как они не обеспечивают критические процессы?	Нет, согласно представленному контексту, объекты критической информационной инфраструктуры (КИИ) должны быть включены в перечень объектов КИИ, даже если они не обеспечивают критические процессы.	Да, возможны ситуации, когда объекты критической информационной инфраструктуры Российской Федерации (КИИ) существуют, но не подлежат включению в Перечень объектов КИИ в соответствии с Федеральным законом № 187-ФЗ. Однако, такие объекты должны быть определены Правительством Российской Федерации.	Согласно представленному контексту, объекты критической информационной инфраструктуры (КИИ) должны быть включены в перечень объектов КИИ, даже если они не обеспечивают критические процессы.	Да, такие ситуации возможны, в зависимости от того, какие процессы автоматизирует объект критической информационной инфраструктуры (далее – КИИ).	Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) _Об утверждении Правил катег
7	Допускается ли выделение отдельных сотрудников, ответственных за обеспечение безопасности ЗОКИИ, в рамках общего структурного подразделения по ИБ?	Да, допускается выделение отдельных сотрудников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры, в рамках общего структурного подразделения по информационной безопасности.	Да, руководитель субъекта критической информационной инфраструктуры может выделить отдельных сотрудников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры, в рамках общего структурного подразделения по информационной безопасности. Структурное подразделение по информационной безопасности не может выполнять функции, не связанные с обеспечением безопасности значимых объектов критической информационной инфраструктуры или обеспечением информационной безопасности субъекта критической информационной инфраструктуры в целом.	Да, допускается выделение отдельных сотрудников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры, в рамках общего структурного подразделения по информационной безопасности.	Да, допускается возложение функций по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ) на отдельных сотрудников подразделения по информационной безопасности: · согласно пункту 10 Требованиям к созданию систем безопасности значимых объектов КИИ, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 (далее – Требования к СОИБ), допускается назначение отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ; · согласно пункту 13 Требованиям к СОИБ, сотрудники, ответственные за обеспечение безопасности значимых объектов КИИ, могут выполнять функции, связанные с обеспечением информационной безопасности субъекта КИИ в целом.	Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) _Об утверждении Требованиям к созданию с
8	Установлен ли законодательством шаблон Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (приказ ФСБ России № 282)?	Нет, законодательством не установлен шаблон плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак.	Нет, законодательство не устанавливает шаблона Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак.	Да, законодательством не установлен шаблон плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак.	Нет, шаблон плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее – План) законодательно не установлен.	Приказ ФСБ России от 19.06.2019 № 282 (ред. от 07.07.2022) _Об утверждении Порядка информирования ФС
9	Являются ли транспортные средства и (или) их отдельные компоненты объектами КИИ?	Нет, транспортные средства и (или) их отдельные компоненты не являются объектами критической информационной инфраструктуры.	Нет, транспортные средства и (или) их отдельные компоненты не являются объектами критической информационной инфраструктуры.	Да, транспортные средства и (или) их отдельные компоненты являются объектами критической информационной инфраструктуры.	Сами транспортные средства не являются объектами КИИ, а их отдельные компоненты могут быть отнесены к объектам КИИ, в случае если данные компоненты являются составной частью АСУ и ИС.	Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) _О безопасности критической информацио
10	При внесении изменений в План реагирования на компьютерные инциденты, необходимо ли новую версию плана направлять в НКЦКИ?	Да, при внесении изменений в План реагирования на компьютерные инциденты, новую версию плана необходимо направлять в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).	Да, если в план реагирования на компьютерные инциденты были внесены изменения, то необходимо направить новую версию плана в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).	Да, при внесении изменений в План реагирования на компьютерные инциденты, новую версию плана необходимо направлять в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).	После утверждения Плана руководителем субъекта критической информационной инфраструктуры (далее – КИИ), копия утвержденного Плана в течение 7 календарных дней со дня утверждения направляется в НКЦКИ в соответствии с абзацем 6 пункта 6 Порядка информирования. В данный План, согласно пункту 10 Порядка информирования, при необходимости по результатам тренировок по отработке мероприятий Плана (проводятся не реже раза в год) могут вноситься изменения. Соответственно, План меняется и должен быть утвержден руководителем субъекта КИИ, после чего копия утвержденного Плана также в течение 7 календарных дней со дня утверждения руководителем субъекта КИИ направляется в НКЦКИ.	Приказ ФСБ России от 19.06.2019 № 282 (ред. от 07.07.2022) _Об утверждении Порядка информирования ФС
11	Является ли компьютерным инцидентом целенаправленное (преднамеренное) нарушение правил эксплуатации объекта КИИ?	Да, целенаправленное (преднамеренное) нарушение правил эксплуатации объекта КИИ является компьютерным инцидентом.	Да, преднамеренное нарушение правил эксплуатации объекта КИИ является компьютерным инцидентом. Компьютерный инцидент может привести к нарушению функционирования объекта КИИ.	Да, целенаправленное (преднамеренное) нарушение правил эксплуатации объекта КИИ является компьютерным инцидентом.	Если нарушение правил эксплуатации объекта КИИ привело к нарушению функционирования или безопасности объекта КИИ, то такое действие следует рассматривать как компьютерный инцидент.	Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) _О безопасности критической
12	Будет ли действовать сертификат соответствия СрЗИ при использовании функций безопасности, не указанных в документации на СрЗИ?	Нет, сертификат соответствия СрЗИ будет действителен только для функций безопасности, указанных в документации на СрЗИ.	Нет информации для ответа на данный вопрос.	Сертификат соответствия СрЗИ будет действителен только для функций безопасности, указанных в документации на СрЗИ. Использование функций безопасности, не указанных в документации на СрЗИ, может привести к нарушению требований безопасности и недействительности сертификата соответствия.	Действие сертификата соответствия требованиям по безопасности, выданный на определенное средство защиты информации (далее – СрЗИ), не будет приостановлено, но он не распространяется на те функции безопасности, которые не указаны в соответствующем сертификате.	Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) _Об утверждении Требованиям по обеспечен

13	Обязательно ли создание отдельной системы менеджмента (управления) безопасности объектов КИИ или допускается интегрированная СМИБ, включающая процессы управления безопасностью как объектов КИИ, так и других объектов защиты?	Создание отдельной системы менеджмента (управления) безопасности объектов КИИ является обязательным. Допускается интеграция этой системы с другими системами менеджмента (управления), но только если это не противоречит требованиям законодательства Российской Федерации.	Да, создание отдельной системы менеджмента (управления) безопасности объектов КИИ обязательно. Однако, допускается интеграция этой системы с другими системами менеджмента (управления), если это не противоречит требованиям законодательства Российской Федерации.	Создание отдельной системы менеджмента (управления) безопасности объектов КИИ является обязательным. Допускается интеграция этой системы с другими системами менеджмента (управления), но только если это не противоречит требованиям законодательства Российской Федерации.	Нет, не обязательно.	Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) _Об утверждении Требований к созданию с
14	Возможно ли изменения категории значимости, определенной на стадии технического задания создаваемого объекта КИИ (например, в рамках его проектирования или внедрения)?	Да, возможно изменение категории значимости, определенной на стадии технического задания создаваемого объекта КИИ. Это может произойти, например, в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого он перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости. Также изменение категории значимости возможно в случае ликвидации, реорганизации субъекта критической информационной инфраструктуры и (или) изменения его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.	Да, возможны.	Да, возможно изменение категории значимости, определенной на стадии технического задания создаваемого объекта КИИ. Это может произойти, например, в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого он перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости. Также изменение категории значимости возможно в случае ликвидации, реорганизации субъекта критической информационной инфраструктуры и (или) изменения его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.	Да. Категория значимости может быть пересмотрена в зависимости от фактических показателей критериев значимости, угроз безопасности информации, взаимодействия с иными объектами критической информационной инфраструктуры (далее – КИИ) и (или) иной информации, указанной в пункте 10 Правил категорирования. Решение о пересмотре категории значимости принимает комиссия по категорированию с учетом текущих и (или) планируемых условий эксплуатации объекта КИИ.	Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) _Об утверждении Правил катег
15	Требуется ли дополнительно к оценке основных функций безопасности проводить оценку соответствия несертифицированного, но встроенного в общесистемное или прикладное ПО средства защиты информации по оценочному уровню доверия?	Нет, дополнительная оценка соответствия не требуется.	Оценка безопасности критической информационной инфраструктуры осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной информации;	Дополнительная оценка соответствия не требуется.	Нет, дополнительная оценка соответствия по оценочному уровню доверия для несертифицированных средств защиты информации (далее – СрЗИ), встроенных в общесистемное или прикладное программное обеспечение (далее – ПО), не требуется.	Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) _Об утверждении Требований по обеспечен
16	Является ли «Служба спасения» субъектом КИИ?	Нет, «Служба спасения» не является субъектом КИИ.	Нет, «Служба спасения» не является субъектом КИИ. Категория значимости, к которой может быть отнесена «Служба спасения», может быть первой.	«Служба спасения» не является субъектом КИИ.	Нет, не является.	Постановление Правительства РФ от 30.12.2003 № 794 (ред. от 17.01.2024) _О единой государственной си
17	Относятся ли сайты субъектов КИИ к объектам КИИ?	Да, сайты субъектов КИИ относятся к объектам КИИ.	Да, согласно представленному контексту, сайты субъектов критической информационной инфраструктуры могут быть отнесены к объектам критической информационной инфраструктуры. Информационные системы субъектов критической информационной инфраструктуры также относятся к объектам критической информационной инфраструктуры.	Сайты субъектов КИИ относятся к объектам КИИ.	Сайты являются частью информационных систем (далее – ИС) и они не могут быть самостоятельными объектами критической информационной инфраструктуры (КИИ), но могут быть функциональной частью таких объектов.	Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) _Об информации, информационных техноло
18	Если у иностранной компании имеется филиал в России, распространяется ли 187-ФЗ на него?	Да, если у иностранной компании имеется филиал в России, то на него распространяется действие 187-ФЗ.	Да, действие Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" распространяется на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, которые принадлежат государственным органам, государственным учреждениям, российским юридическим лицам и (или) индивидуальным предпринимателям на праве собственности, аренды или на ином законном основании.	Да, если у иностранной компании имеется филиал в России, то на него распространяется действие 187-ФЗ.	Нет, не распространяется.	Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) _О безопасности критической информации
19	Требуется ли оценка соответствия СрЗИ, не включенных в базовый набор мер защиты (239 приказ ФСТЭК), но используемых для обеспечения безопасности ЗОКИИ?	Да, требуется оценка соответствия СрЗИ, не включенных в базовый набор мер защиты (239 приказ ФСТЭК), но используемых для обеспечения безопасности ЗОКИИ.	Да, требуется оценка соответствия средств защиты информации, не включенных в базовый набор мер защиты (239 приказ ФСТЭК), но используемых для обеспечения безопасности значимого объекта критической информационной инфраструктуры.	Да, требуется оценка соответствия СрЗИ, не включенных в базовый набор мер защиты (239 приказ ФСТЭК), но используемых для обеспечения безопасности ЗОКИИ.	СрЗИ, не включенные в базовый набор мер защиты для соответствующей категории значимого объекта КИИ, подлежат оценке соответствия в случае, если они применяются для адаптации, дополнения или комбинирования базового набора мер и определены в рамках технического задания и технического проекта на подсистему безопасности значимого объекта КИИ. При использовании таких СрЗИ для реализации вспомогательных и (или) прикладных функциональных целей оценка соответствия не требуется.	Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) _Об утверждении Требований по обеспечен
20	Если сферу образования включают в ст. 2 187-ФЗ, то означает ли, что школы станут субъектами КИИ?	Нет, это не означает, что школы станут субъектами КИИ. Статья 2 Федерального закона № 187-ФЗ определяет основные понятия, используемые в данном законе, но она не включает сферу образования.	Если сферу образования включают в статью 2 Федерального закона № 187-ФЗ, то это не означает, что школы станут субъектами КИИ. Субъектами КИИ являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним.	Если сфера образования будет включена в статью 2 Федерального закона № 187-ФЗ, то это не означает, что школы станут субъектами КИИ. Статья 2 данного закона определяет основные понятия, используемые в законе, но она не включает сферу образования.	Да, образовательные учреждения, включая школы, станут субъектами критической информационной инфраструктуры.	Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) _О безопасности критической информации