Вебинар 05.12.2023

Информационная безопасность объектов КИИ –
от категорирования до построения системы защиты и импортозамещения

ВОПРОС	ОТВЕТ
Хотелось бы узнать вашу точку зрения на различия между ИТКС и сетью электросвязи. На мой взгляд, сеть электросвязи более широкое понятие и включает ИТКС. Есть ли рекомендации в каких случаях объект считать ИТКС, а в каких - сетью электросвязи?	**Сети электросвязи** - технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания. Согласно п.1 статьи 12 ФЗ № 126 "О связи" **единая сеть электросвязи** РФ состоит из расположенных на территории РФ сетей электросвязи следующих категорий: сеть связи общего пользования; выделенные сети связи; технологические сети связи, присоединенные к сети связи общего пользования; сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем. Согласно п. 4 статьи 3 ФЗ № 149 "Об информации, информационных технологиях и о защите информации" **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. В случае выделения ИТКС (например, ЛВС) субъекта КИИ в качестве объекта КИИ, данный объект КИИ стоит рассматривать как ИТКС, подключенной к сети электросвязи. Сеть электросвязи как объект КИИ выделять не нужно. При проведении категорирования необходимо указать, что ОКИИ имеет подключение к сети электросвязи (в случае наличия подключения).
Согласно Указу №250 до 2025 года необходимо перейти на отечественное ПО. Вопрос: как это реализовать на промышленном оборудовании (ЧПУ) с ОС Windows XP и прочих.	Рекомендуем ознакомиться с Постановлением Правительства РФ от 22.08.2022 N 1478 (ред. от 17.10.2023) "Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц"

	(за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации".
Вот это вот: ОКВЭД и ОКОГУ, лицензии, сертификаты в пункте первом откуда взяты? сами придумали или есть какой-то нормативный акт?	Процедура определения сферы деятельности организации по ОКВЭД и т.п. не регламентирована в НПА. На основании данной информации нельзя определить принадлежность организации к субъектам КИИ (это было озвучено спикерами в рамках вебинара). Данную информацию предлагает использовать ФСТЭК России и отраслевые регуляторы как вспомогательную.
Мнение ФСТЭК по ОКВЭД это мнение, они не смогли предоставить обоснованность такого шага. Вам они какое-то юридическое обоснование своего мнения предоставили?	Процедура определения сферы деятельности организации по ОКВЭД и т.п. не регламентирована в НПА. На основании данной информации нельзя определить принадлежность организации к субъектам КИИ (это было озвучено спикерами в рамках вебинара). Данную информацию предлагает использовать ФСТЭК России и отраслевые регуляторы как вспомогательную.
Что включается в состав ИС/АСУ/ИТКС?	1) **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. В состав ИС включаются технические средства (АРМ, серверы, СХД и т.д.), обрабатывающие информацию, программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), СЗИ. 2) **Автоматизированная система управления** - автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами. В состав АСУ включается программно-технический комплекс, включающий технические средства (в том числе АРМ, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), а также СЗИ. 3) **Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. В состав ИТКС включается сетевое оборудование (коммутаторы, маршрутизаторы и т.п.), каналы связи, СЗИ.

Слово "Функционирующие" в термины субъекты КИИ, вы к чему относите к объектам или к субъектам?	К объектам.
Как поступать с объектами, чьи категории не выше третьей, но если атака будет одновременной сразу на несколько из них, то ущерб может наступить как у 2-й или даже 1-й категории?	Рекомендуем при категорировании рассматривать наихудшие сценарии в результате проведения целенаправленных компьютерных атак, в том числе такие как одновременные атаки на все ОКИИ.
Вопрос по категорированию: зачастую, особенно вначале действия 187-ФЗ, субъекты КИИ из-за отсутствия опыта и разъяснений регулятора направляли во ФСТЭК России сведения о признании значимыми объектов КИИ, которые по сути к таковым не относятся. Регулятор же, как правило, все одобрял и вносил в реестр сведения о ЗОКИИ на объекты, которые, по сути, таковыми не являются (в качестве примере - холодный биллинг у оператора связи). Вопрос: имеется ли практика "раскатегорирования" ЗОКИИ, и каков порядок? Нужны ли предварительные согласования со ФСТЭК России?	Да, у нашей компании есть практика по оказанию помощи субъектам КИИ в части исключения ошибочно признанных значимыми объектов КИИ. Для этого необходимо оформить протокол заседания постоянно действующей комиссии, в котором отразить результаты пересмотра полученных значений по каждому из рассчитываемых показателей критериев значимости или информацию о неприменимости показателя к объекту (обязательно максимально аргументированно), признать ранее допущенную ошибку. Далее отправить регулятору протокол, новые сведения по форме из 236 приказа ФСТЭК. В сопроводительном письме указать на ранее допущенную ошибку и попросить исключить ОКИИ из реестра ЗОКИИ.
Вопрос по категорированию ЦОД. Если на базе инфраструктуры ЦОД развернуты ИС разных организаций, и являющиеся ОКИИ, нужно ли оператору ЦОД проводить категорирование и как происходит разграничение, когда ЦОД является КИИ и когда нет?	Если организация - владелец ЦОД не является субъектом КИИ, то размещение в ЦОД ИС, являющихся ОКИИ, не является основанием признавать организацию-владельца ЦОД субъектом КИИ, т.к. данные ИС им не принадлежат. Соответственно проводить категорирование ЦОД не требуется.
Надо ли основании ваших рассуждений про производителя лекарств аналогично отнести к субъектам КИИ все десятки тысяч	Да, аптека является субъектом КИИ если ей принадлежит ИС, функционирующая в сфере здравоохранения.

розничных аптек - они тоже осуществляют фармацевтическую деятельность и имеют как минимум товароучетную систему - ИС?	
А кадровый учет (1С: Зарпалта и кадры) в какой сфере деятельности функционирует? непонятно логика вашего мышления	Если хотя бы одна система организации функционирует в сфере из 187-ФЗ, то все остальные ИС/АСУ/ИТКС являются объектами КИИ согласно определению объекта КИИ из 187-ФЗ. Кадровый учет (1С: Зарпалта и кадры) субъекта КИИ может не функционировать в соответствующей сфере из 187-ФЗ, но она всё равно будет являться объектом КИИ, т.к. она принадлежит субъекту КИИ.
При публикации отраслевого перечня объектов КИИ ОБЯЗАТЕЛЬНО необходимо пересмотреть перечень?	Да, необходимо как минимум свериться с перечнем и при необходимости прокатегорировать те ОКИИ, которые фигурируют в перечне и ранее не были включены в перечень ОКИИ, подлежащих категорированию (при наличии таковых).
Где можно найти типовые перечни КИИ?	Разработка типовых перечней объектов КИИ возложена на отраслевых регуляторов. Если на официальном сайте отраслевого регулятора типовой перечень отсутствует, советуем запросить его письменно. Отметим, что на текущий момент официально опубликованы в открытом доступе типовые перечени только в сфере транспорта и энергетики.
Допустимо ли объединение нескольких объектов КИИ в один?	Да, возможно, в случае если данные ОКИИ обеспечивают один технологический процесс и включают в себя идентичное оборудование.
Является ли самолет или корабль объектом КИИ?	Самолет или корабль сами по себе не являются ИС/АСУ/ИТКС, поэтому не могут являться объектами КИИ, но совокупность бортового и наземного оборудования в составе АСУ самолета или корабля вполне могут быть объектами КИИ, функционирующими в сфере транспорта.
У нас тут лицензиат заходил и категорировал локальную сеть как объект КИИ, в акте не указано юридическое объяснение. Как вы категорируете локальную сеть? Совершаете ли такие действие в отношении такого объекта и как юридически обосновываете такое действие.	Мы в своей практике используем два варианта: 1) ЛВС выделяется как отдельный объект КИИ (ИТКС), в состав которого включается сетевое оборудование и каналы связи. Данный подход используется преимущественно в тех сферах, где в отраслевых требованиях по ИБ есть требования по выделению ЛВС в качестве отдельного ОКИИ 2) ЛВС как отдельный ОКИИ не выделяется, но всё оборудование, функционирующее в составе ЛВС включается в состав других ОКИИ, взаимодействие которых обеспечивает ЛВС.
Каждый сервер — это объект КИИ? Или объект КИИ совокупность ИС относящиеся к процессу компании?	Объектом КИИ является ИС, а сервер — это средство вычислительной техники, которое входит в состав ИС.

Почему ЦБ для определения значимости ОКИИ по п. 10.4 (ПП-127) считает, что нужно оценивать объемом всех активов (млрд. рублей) организации, хотя в случае КА и КИ на ИС (ОКИИ) по факту не приведет к последствиям в размере всех активов. Как им это обосновать.	Разъяснение подходов ЦБ в части категорирования ОКИИ, к сожалению, не в наших компетенциях. Можем только посоветовать попробовать в результатах категорирования более подробно обосновать, что КА и КИ на ИС (ОКИИ) не приведет к последствиям в размере всех активов (если это действительно так).
Критические процессы — это процессы, без которых компания не выживет или это процессы, влияющие на государство?	Критическими являются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) **прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка**.
Модель угроз должна разрабатываться для значимых объектов КИИ согласно приказам ФСТЭК. Значимый объект определяется по результатам категорирования, которое в свою очередь требует наличия модели угроз. Что первично?	На этапе категорирования достаточно определить только перечень основных угроз безопасности информации для ОКИИ, разрабатывать модель угроз не обязательно и не требуется в соответствии с НПА. Разработка модели угроз для ЗОКИИ обязательна согласно требованиям приказа ФСТЭК № 239, она разрабатывается после признания ОКИИ значимым.
Если нет категории значимости, нужно информировать ФСТЭК о проведении категорирования?	Да, согласно п. 17 ПП РФ № 127 - субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 16 настоящих Правил, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости **либо об отсутствии необходимости присвоения ему одной из таких категорий**.
При анализе ПАК на доверенность, насколько низкоуровневое ПО нужно рассматривать?	Согласно ПП РФ № 1912 - "программно-аппаратный комплекс" - радиоэлектронная продукция, в том числе телекоммуникационное оборудование, **программное обеспечение** и технические средства, работающие совместно для выполнения одной или нескольких сходных задач. Опираясь на данное определение можем предположить, что необходимо рассматривать всё ПО, функционирующее в составе ПАК. Также заметим, что данный НПА достаточно новый и надеемся, что в ближайшее время могут появиться разъяснения от регуляторов, в том числе отраслевых.

Я правильно понимаю, то ПП-1912 касается только ЗО КИИ?	Верно.
ЛВС обязательно выделять в качестве отдельного объекта КИИ?	Мы в своей практике используем два варианта: 1) ЛВС выделяется как отдельный объект КИИ (ИТКС), в состав которого включается сетевое оборудование и каналы связи. Данный подход используется преимущественно в тех сферах, где в отраслевых требованиях по ИБ есть требования по выделению ЛВС в качестве отдельного ОКИИ 2) ЛВС как отдельный ОКИИ не выделяется, но всё оборудование, функционирующее в составе ЛВС включается в состав других ОКИИ, взаимодействие которых обеспечивает ЛВС.
Как защищать объект КИИ, в составе которого нет АРМ и серверов?	1) Защита периметра ОКИИ (в случае подключения ОКИИ к ЛВС или сети "Интернет) 2) Использование встроенных функций по ИБ прикладного и системного ПО ОКИИ 3) Применение организационных, компенсирующих мер
И нужно ли повторно отправлять во ФСТЭК перечень объектов КИИ по результатам категорирования нового объекта КИИ?	Нет, перечень объектов КИИ, подлежащих категорированию, отправляется регулятору единожды. По результатам категорирования нового объекта КИИ регулятору направляется только сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
Для услуги по проектированию в защищенном исполнении ЛИЦЕНЗИЯ ФСТЭК НЕ НУЖНА если для собственных нужд!	Данное утверждение не соответствует требованиям НПА. Посмотрите, пожалуйста, требования ПП РФ № 79. Те пункты, где фигурируют «работы» — нужна лицензия даже для собственных нужд - пункты г) и д). Те пункты, где фигурируют «услуги» — нужна лицензия только для оказания таких услуг сторонним организациям, для собственных нужд лицензия не требуется.
Объект КИИ, который еще не введен в эксплуатацию, подлежит категорированию?	Да, согласно п. 8 ПП РФ № 127 - в отношении создаваемого объекта критической информационной инфраструктуры, в том числе в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных о критических процессах субъекта критической информационной инфраструктуры. Для создаваемого объекта критической информационной инфраструктуры, указанного в абзаце первом настоящего пункта, категория значимости может быть уточнена в ходе его проектирования.

Возможны бесплатные консультации для новых территорий у которых не то что ноль, а минус 100 по КИИ, ПДн, ГИС?	По данному вопросу с Вами свяжутся наши региональные менеджеры.
Возможно ли вам передать в управление вопросы ИБ или вы можете предоставить сотрудника для контроля актуализации документов работы с ДЛП а так же проводить обучение персонала.	Да, это возможно. По данному вопросу с Вами свяжутся наши региональные менеджеры.