Категорирование объектов КИИ

Как обычно, принятие новых законодательных актов, с целью усиления контроля, через некоторое время вызывает у предприятий обязанность создания и направление в уполномоченные государством органы новой отчетной документации, что всегда приводит к рождению «фирмочек», якобы аккредитованных этими органами, предлагающих за немалые деньги «разработку» этой документации для предприятий. Вспомним: документы для лицензирования, ПВК, включение в реестр ЦБ РФ и т. П. Но сейчас «ценовой рекорд» побит стоимостью категорирования объектов КИИ – от 100 тыс руб.

Лига ломбардов изначально боролась с такими «помощниками» бесплатно предлагая своим участникам подлежащие редактированию ими «шаблоны» или, по крайне мере, разъяснения несложную методику самостоятельной разработки таких документов. Соблюдаем этот порядок в очередной раз.

Общие понятия

Субъект – это Ваше предприятие: ломбард или Хранитель.

Объект КИИ – это информационная система -ИС информационно-телекоммуникационная сеть — ИТС АСУТП — автоматизированная система управления.

В нашем случае это ИС — это база данных, ИТС- интернет, ПО, обеспечивающее автоматизацию деятельности ломбарда -АСУТП.

В настоящем материале в качестве примера АСУТП рассматривается АСУТП «Ломбард» разработки ООО Фирма «Техноломбардсервис-2», отличительной особенностью которой является обезличивание сведений о предмете вещи залога (поклажи) и присвоение ей уникального ID уже на первом этапе обработки данных и автономность каждого объекта КИИ (его независимость от наличия Интернета). Таким образом, информация, относящаяся к основному признаку критичности инфраструктуры – персональным и имущественным данным субъектов защиты – потребителей услуг ломбарда (Хранителя) по телекоммуникационным сетям не передается). Возможность идентификации владельца заложенной или сданной на хранение вещи доступна только уполномоченным работником подразделения, в котором используется АСУТП.

По телекоммуникационным сетям между подразделениями и сервером субъекта передается интегрированная информация уже распределенная по регистрам бухгалтерского, налогового и управленческого учета, за

исключением информации, передаваемой на основании законодательства РФ в Банк России и ГИИС ДМ ДК по защищенным и сертифицированным каналам связи.

К сожалению, Лига ломбардов не имеет достаточной информации о защищенности информации предприятий, использующих другие многочисленные виды ПО. Поэтому рекомендуем провести с Вашим IT вендером консультации по вопросу безопасности информации, содержащей конфиденциальную информацию.

Основная задача предприятия по категорированию.
На основании Постановления Правительства № 127 предоставить сведения по форме, утвержденной приказом ФСТЭК России от 22 декабря 2017г № 236 в редакции от 31 марта 2019г **обосновать** ОТСУТСТВИЕ НЕОБХОДИМОСТИ присвоение предприятию одной из категорий значимости КИИ, для чего создать

Документы, предоставляемые ФСТЭК:

1. Приказ о создании комиссии для категорирования значимости объектов КИИ

Образец

Москва 2025г

Приказ БН от _____

В целях исполнения Закона № 187-ФЗ

Приказываю:

Создать комиссию по категорированию значимости объектов КИИ (АСУТП и ИТС, используемых подразделениями предприятия в составе членов комиссии:

Председатель комиссии____
Директор ООО/ИП_____

2. Акт категорирования объектов КИИ, используемых подразделениями _____(наименование предприятия)
А) Мы, нижеподписавшиеся члены комиссии по категорированию объектов КИИ, созданной в соответствии с Приказом от_____ №___ составили и утвердили настоящий акт о том, что во всех подразделениях используются объекты КИИ, не содержит отличных от нуля значений по каждому из пяти критериев в информации. Сведения об отсутствии необходимости присвоения идентичным объектом КИИ одной из категорий значимости

содержатся в прилагаемой таблице, утвержденной Приказом ФСТЭК России от 22 декабря 2017г № 236 (с изменениями от 21 марта 2019г).
Члены комиссии: _____(ФИО, дата)
_____(ФИО, дата)
Председатель: _____(ФИО, дата)
Печать предприятия
Б)

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Ограничительная пометка или гриф секретности (при необходимости)

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
1.4.	Назначение объекта	
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктур

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2.	Наименование оператора связи и (или) провайдера хостинга	
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим,	

	производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное	

	программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости

8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	

8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	

_____	_____	_____
(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)	(подпись)	(инициалы, фамилия)
	М.П. (при наличии печати)	

"__" _____ 20___ г.

Рекомендации по заполнению таблицы

1.1 Наименование Вашего ПО
1.2 Адреса Ваших подразделений
1.3 Деятельность ломбарда/услуги по хранению имущества (для Хранителя)
1.4 Обеспечение автоматизированного учета и контроля всех операций предприятия, передача данных структурам, законодательно уполномоченным к их получению
1.5 ИС, ИТС, АСУТП
1.6 Распределенная система управления
2.1 Ваш юридический адрес
2.2 Ваш адрес местонахождения (управления)
2.3, 2.4 Директор

2.5 Отсутствует
2.6 Указать ИНН предприятия, КПП – при наличии
3.1 Указать тип сети
3.2 Указать провайдера
3.3 Обмен обработанной информацией между подразделениями и сервером субъекта в структуры, в порядке установленном законодательством.
3.4 Беспроводной
4.1, 4.2 Указать данные
4.3 Все указанные элементы
4.4 Повторить пункт 2.6
5.1 Наименование используемого ПО, договор с провайдером
5.2 Уточнить у IT вендера
5.2 1С
5.4 Информация, являющаяся подлежащей защите находится на жестких дисках компьютеров, находящихся в помещениях подразделений, технически укрепленных и поставленных на охрану предприятием____, имеющим соответствующую лицензию №_____. Доступ в помещение предоставлен только работникам подразделения и лицам, уполномоченным руководителям субъекта КИИ или законом.
Доступ к ИС (элементу АСУТП) возможен исключительно по паролю работника, известному только ему (далее для пользователей АСУТП разработки ООО Фирмой Техноломбардсервис-2). Доступ к ключу ИС снабжен функцией самоуничтожения ключа в случае несанкционированного доступа в систему, подлежит восстановлению только фирмой – разработчиком, с составлением соответствующего акта (протокола).
Информация, передаваемая на основании законодательства в ЦБ РФ и ГИИС ДМ ДК защищена сертифицированными средствами защиты, применяемые этими структурами.
6.1 Нарушение (взлом) ИТС не приведет к утечке предмета критичности информации – персональным и имущественным данным потребителей в связи с невозможностью идентификации субъекта конфиденциальных данных (для пользователей АСУТП разработки ООО Фирмой Техноломбардсервис-2). Передаваемые данные не предъявляют при их утечке угроз предпринимательской деятельности субъектам КИИ.
6.2 Основную угрозу безопасности информации представляется передача информации о потребителе криминальным структурам.
7.1 Передача информации от объекта КИИ субъекту осуществляется с периодичностью, определяемой по воле оператора ПО объекта, пакетами, содержащими информацию за установленные им периоды (далее для АСУТП

разработки ТЛС-2). Вероятность определения момента передачи ничтожна, соответственно ничтожна вероятность компьютерного инцидента по этой причине. Автономностью создания и передачи объектом КИИ обусловлена независимость передачи информации отказа в обслуживании и даже отсутствия энергоснабжения. Подразделение субъекта КИИ может достаточно долго работать « в ручном режиме» с последующим вводом в ПО рукописных данных и передачи итогов их обработки субъекту КИИ.

Невозможность несанкционированного доступа модификации данных и других возможностей компьютерных инцидентов изложена в п. 5.4 таблицы.

Защита от утечки данных, связанная с действиями работников объекта КИИ или несанкционированное использования технических средств (в том числе вычислительных ресурсов объекта) осуществляется административными способами (см далее).

8.1 Решение комиссии, созданной приказом по субъекту КИИ установлено несоответствие объектов КИИ предприятия ни одной из категорий значимости, и соответственно о неприсвоении объектам ни одной из таких категорий.

8.2 Значение по каждому из 5 показателей критериев значимости КИИ по отношению к объектам используемого ПО равно нулю.

8.3 Нулевые значения показателей очевидны.

9.1 Организационные меры установлены в трудовом договоре работника и субъекта КИИ. Контроль доступа к АСУТП обеспечен протоколированием временным входом и физического лица, осуществляющего вход в АСУТП. Со всеми работниками предприятия проведен инструктаж о соблюдении конфиденциальности информации в соответствии с Законами № 196-ФЗ. Все работники информированы об ответственности за утечку конфиденциальных сведений. Копия протокола проведения инструктажа прилагается.

9.2 Программная среда объектов КИИ использует антивирусную защиту Касперского.

Примечание

Предприятиям, использующим ПО, отличное от АСУТ «Ломбард» для заполнения пунктов 5.4, 7.1, 9.1 следует получить от IT вендеров ПО, которые они используют, сведения о защите информации, которой обмениваются компьютерная система по сети Интернет в части конфиденциальной информации, документы о сертификации в частности облачных сервисов.

3. Протокол

О проведении инструктажа работников___ по соблюдению законодательства Российской Федерации по защите конфиденциальной информации.

_____ августа 2025г был проведен инструктаж о соблюдении конфиденциальности информации в соответствии с Федеральными законами: № 126-ФЗ, № 196-ФЗ и №187-ФЗ. Все инструктируемые работки предупреждены об ответственности за утечку информации, установленной указанными законами, что засвидетельствовано собственноручными подписями.

Должность, ФИО, подпись, дата
Старший товаровед Петрова Ирина Ивановна

Инструктаж провел_____(должность, ФИО, подпись)
Протокол утверждаю ___ (директор, ФИО, подпись)