



Подходы к категорированию объектов КИИ в финансовой отрасли

Взгляд эксперта

Кузнецов Александр, CISM, MVP

Руководитель направления ИБ

20.09.2018

www.ntc-vulkan.ru

Терминология в области КИИ	3
Процесс категорирования «на пальцах»	5
Категорирование в деталях	6
«Путь» от сферы деятельности субъекта КИИ до перечня объектов КИИ	8
«Путь» от перечня объектов КИИ до принятия решения о значимости	24
Заключение	27
Вопросы и ответы	28

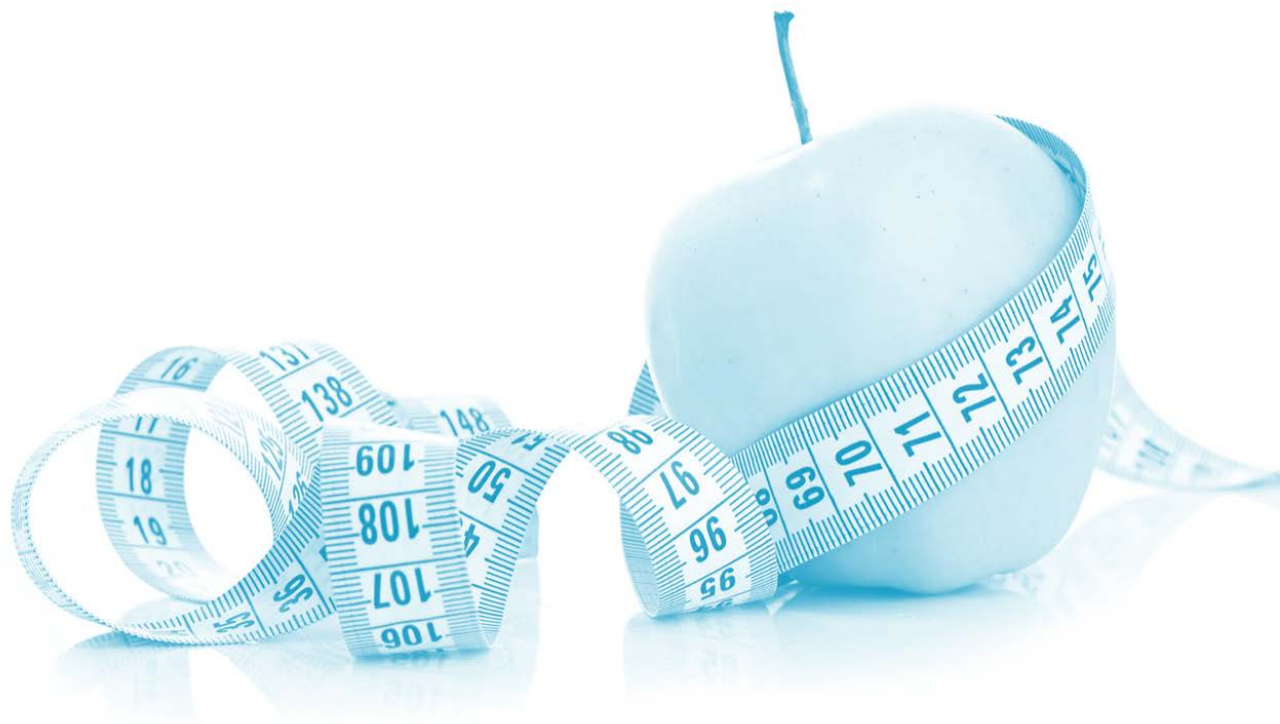
- **Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
- **Значимый объект критической информационной инфраструктуры** – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры
- **Субъекты критической информационной инфраструктуры** – российские юридические лица, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в банковской сфере и иных сферах финансового рынка, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей
- **Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки

Субъекты КИИ: Финансовые организации



Категорирование объекта КИИ:

- **Подготовить** входные данные
- **Оценить** подготовленные данные по перечню, утв. ПП РФ
- **Присвоить** либо **не присвоить** категорию значимости



п.5. Категорирование включает в себя: ...

п.10. Исходными данными для категорирования являются: ...

п.14. Комиссия по категорированию в ходе своей работы: ...

п.16. ... актом, который должен содержать ...

п.17. ... сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают: ...



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 февраля 2018 г. № 127

МОСКВА

Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений

В соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые:

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации;

перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

2. Финансирование расходов, связанных с реализацией настоящего постановления государственными органами и государственными учреждениями, осуществляется за счет и в пределах бюджетных ассигнований, предусмотренных соответствующим бюджетом на обеспечение деятельности субъектов критической информационной инфраструктуры.

Председатель Правительства
Российской Федерации



Д.Медведев

3627530

Форма, утв. приказом ФСТЭК России №236

[illegible]

«Путь» от сферы деятельности субъекта КИИ до перечня объектов КИИ

- **Сфера:** банковская сфера и иные сферы финансового рынка
- **Виды деятельности:** ???
- **Процессы:** ???
- **Критические процессы:** ???
- **Объекты КИИ:** ???



Виды деятельности: Операции

Привлечение денежных средств физических и юридических лиц во вклады...



Осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам



Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств..



Размещение привлеченных средств от своего имени и за свой счет



Выдача банковских гарантий



Открытие и ведение банковских счетов физических и юридических лиц



Инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц



Купля-продажа иностранной валюты в наличной и безналичной формах



Привлечение драгоценных металлов физических и юридических лиц во вклады ..., за исключением монет из драгоценных металлов



Виды деятельности: Сделки

Выдача поручительств за третьих лиц, предусматривающих исполнение обязательств в денежной форме



Приобретение права требования от третьих лиц исполнения обязательств в денежной форме



Лизинговые операции



Доверительное управление денежными средствами и иным имуществом по договору с физическими и юридическими лицами



Осуществление операций с драгоценными металлами, монетами из драгоценных металлов в соответствии с законодательством Российской Федерации



Предоставление в аренду физическим и юридическим лицам специальных помещений или находящихся в них сейфов для хранения документов и ценностей

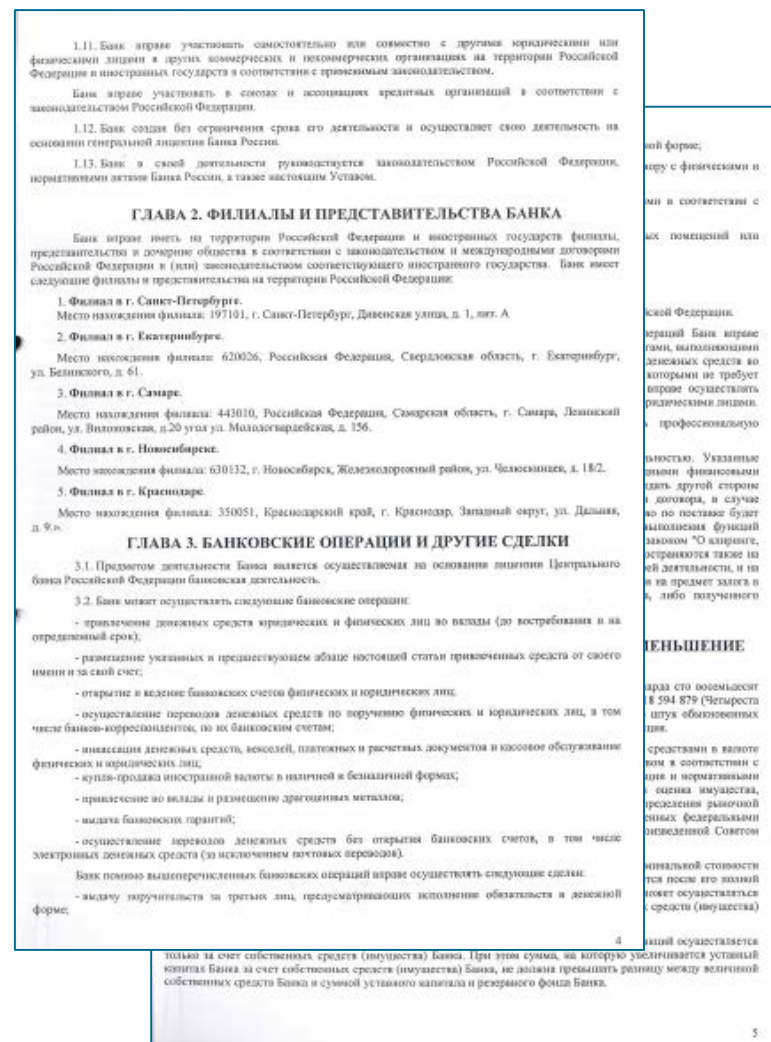


Оказание консультационных и информационных услуг



Источник: Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности»

Виды деятельности: Примеры (начало)



Источники: <https://absolutbank.ru/> и <http://www.cbr.ru>

Виды деятельности: Примеры (окончание)

• ОКВЭД 64.хх

Деятельность по предоставлению финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению

Сведения о видах экономической деятельности по Общероссийскому классификатору видов экономической деятельности (ОКВЭД ОК 029-2014 КДЕС. Ред. 2)			
Сведения об основном виде деятельности			
147	Код и наименование вида деятельности	64.19 Денежное посредничество прочее	
148	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2147711003614 18.04.2014	е вида деятельности
Сведения о дополнительных видах деятельности			
1			
149	Код и наименование вида деятельности	64.99.1 Вложения в ценные бумаги	я в ЕГРЮЛ записи,
150	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2077711004523 28.05.2007	ные сведения
2			
151	Код и наименование вида деятельности	64.99.2 Деятельность дилерская	е вида деятельности
152	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2077711000651 22.01.2007	я в ЕГРЮЛ записи,
3			
153	Код и наименование вида деятельности	64.99.4 Заключение свопов, опционов и других срочных сделок	е вида деятельности
154	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2077711000651 22.01.2007	я в ЕГРЮЛ записи,
4			
155	Код и наименование вида деятельности	66.12 Деятельность брокерская по сделкам с ценными бумагами и товарами	е вида деятельности
156	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2077711000651 22.01.2007	я в ЕГРЮЛ записи,

Источник: <https://egrul.nalog.ru/>

От видов деятельности к процессам

Процесс № 0001

...

Процесс № 7349

Процесс ABC

...

Процесс XYZ

А у нас разве
есть процессы?



От видов деятельности к процессам: Примеры

- На базе ваших реестров процессов



- На базе стандартов от



- Процесс управления взаимоотношениями с потребителями
- Процесс осуществления пассивных депозитных операций
- Процесс осуществления безналичных расчетов
- Процесс управленческого учета и отчетности
- ...

- На базе Basel от



Basel Committee on Banking Supervision

BANK FOR INTERNATIONAL SETTLEMENTS

- Процесс «Корпоративное финансирование»
- Процесс «Торговля и продажа»
- Процесс «Розничные банковские операции»
- Процесс «Коммерческие банковские операции»
- ...

От процессов к критическим процессам

Процесс
критичен для
банка?

Нет, процесс критичен в
масштабах страны!



Нарушение и (или) прекращение каких процессов может привести

- к негативным социальным,
- политическим,
- **экономическим,**
- экологическим последствиям,
- последствиям для обеспечения обороны страны, безопасности государства и правопорядка?

III. Экономическая значимость, п. 10

Оцениваемое **среднедневным** (по отношению к числу календарных дней в году) **количеством осуществляемых операций**, (млн. единиц)

- Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета
- Прекращение или нарушение проведения операций, осуществляемых организацией, являющимся системно значимой кредитной организацией¹
- Прекращение или нарушение проведения операций оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем²
- Прекращение или нарушение проведения операций системно значимой инфраструктурной организацией финансового рынка³

Значение показателя		
III категория	II категория	I категория
3 мл.ед. < ущерб ≤ 70 мл.ед.	70 мл.ед. < ущерб ≤ 120 мл.ед.	120 мл.ед. < ущерб

¹ АО ЮниКредит Банк, Банк ГПБ (АО), Банк ВТБ (ПАО), АО «АЛЬФА-БАНК», ПАО Сбербанк, ПАО «Московский Кредитный Банк», ПАО Банк «ФК Открытие», ПАО РОСБАНК, ПАО «Промсвязьбанк», АО «Райффайзенбанк», АО «Россельхозбанк»

² АО КБ «ЮНИСТРИМ», ЗАО «НKK», ООО «ХэндиСолюшенс», ПАО АКБ «Связь-Банк», ООО «Платежная система «Виза», РНКО «Платежный Центр» (ООО), НКО АО НРД, ООО «Таможенная карта», «Мастеркард» ООО, ООО «Мультисервисная платежная система», Банк ВТБ (ПАО), ПАО Сбербанк, КБ «Геобанк» (ООО), ООО «БЭСТ», ООО «Цифровой Платеж», КИВИ Банк (АО)

³ НКО ЗАО «Национальный расчетный депозитарий» и ЗАО АКБ «Национальный Клиринговый Центр»

III. Экономическая значимость, п. 8

Возникновение ущерба субъекту критической информационной инфраструктуры, который является ... организацией с участием государства¹ и (или) стратегическим акционерным обществом ..., оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (**процентов прогнозируемого объема годового дохода по всем видам деятельности**)

Значение показателя		
III категория	II категория	I категория
3 % < ущерб ≤ 10 %	10 % < ущерб ≤ 15 %	15 % < ущерб

¹ Банк России, Внешэкономбанк, АО «Россельхозбанк», РНКБ Банк, АКБ «РОССИЙСКИЙ КАПИТАЛ», АО «МСП Банк», АО РОСЭКСИМБАНК, АО «ГЛОБЭКСБАНК», ПАО АКБ «Связь-Банк», АО «ВБРР», ОИКБ «Русь», Банк ВТБ (ПАО), АК БАРС, ПАО Сбербанк, АКБ «НОВИКОМБАНК», КБЭР «Банк Казани», АО Газпромбанк, Хакасский Муниципальный Банк, АО «Рускобанк» (РНКО «Нарат», ПАО «Крайинвестбанк», Банк ФК Открытие, Генбанк, ТРАСТ, Промсвязьбанк, Автовазбанк, Рост банк)

² Банк ВТБ (ПАО)

III. Экономическая значимость, п. 8

Процентов прогнозируемого годового дохода бюджета

- Федерального бюджета
- Бюджета субъекта РФ
- Бюджета государственных внебюджетных фондов¹

	Значение показателя		
	III категория	II категория	I категория
Снижение доходов федерального бюджета	$0,001 < \text{ущерб} \leq 0,05$	$0,005 < \text{ущерб} \leq 0,1$	более $0,1 < \text{ущерб}$
Снижение доходов бюджета субъекта Российской Федерации	$0,001 < \text{ущерб} \leq 0,05$	$0,05 < \text{ущерб} \leq 0,1$	$0,1 < \text{ущерб}$
Снижение доходов бюджетов государственных внебюджетных фондов	$0,01 < \text{ущерб} \leq 0,5$	$0,5 < \text{ущерб} \leq 1$	$1 < \text{ущерб}$

¹ Пенсионный фонд, Фонд социального страхования, Государственный фонд занятости населения, фонды обязательного медицинского страхования, фонды социальной поддержки населения и др.



Объекты КИИ, которые

- **обрабатывают информацию,** необходимую для обеспечения выполнения критических процессов,
- **осуществляют управление,**
- **контроль**
- **мониторинг критических процессов**

№	Наименование процесса	Функции объекта КИИ			
		Обработка	Управление	Контроль	Мониторинг
1	Процесс А	Объект №1	Объект №4	Объект №4	Объект №4
2	Процесс Б	Объект №2	-	Объект №5	Объект №5
3	Процесс В	Объект №3	-	-	Объект №5

- Автоматизированная банковская система (АБС)
- Система дистанционного банковского обслуживания (СДБО)
- Процессинговая система
- Скоринговая система
- Антифрод система
- Сеть банкоматов
- Сеть платежных терминалов
- Сеть информационных киосков

Перечень объектов КИИ

УТВЕРЖДАЮ

Должность руководителя субъекта критической
информационной инфраструктуры Российской Федерации
(далее – субъект) или уполномоченного им лица

Подпись руководителя
субъекта или уполномоченного
им лица
« ____ » _____ 20__ г.

Фамилия, имя, отчество (при наличии)
руководителя субъекта или
уполномоченного им лица

Дата утверждения перечня объектов критической информационной
инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

N п/п	Наименование объекта	Тип объекта ¹	Сфера (область) деятельности, в которой функционирует объект ²	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии) ³
1.					
2.					
...					
n.					

¹ Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

² Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

³ Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

- Информационное сообщение ФСТЭК России от 24 августа 2018 г. N 240/25/3752

«Путь» от перечня объектов КИИ до принятия решения о значимости

- **Объекты КИИ:** приведены в перечне
- **Действия нарушителей:** ???
- **Угрозы и уязвимости:** ???
- **Масштаб возможных последствий:** ???
- **Значимость:** ???

Вам потребуются:

- Модель угроз
- Модель нарушителя
- Статистические по компьютерным инцидентам



- Рассмотреть **возможные действия нарушителей** в отношении объектов КИИ, а также иные источники угроз безопасности информации

или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации

- Проанализировать угрозы безопасности информации и уязвимости, которые **могут привести к возникновению компьютерных инцидентов** на объектах КИИ

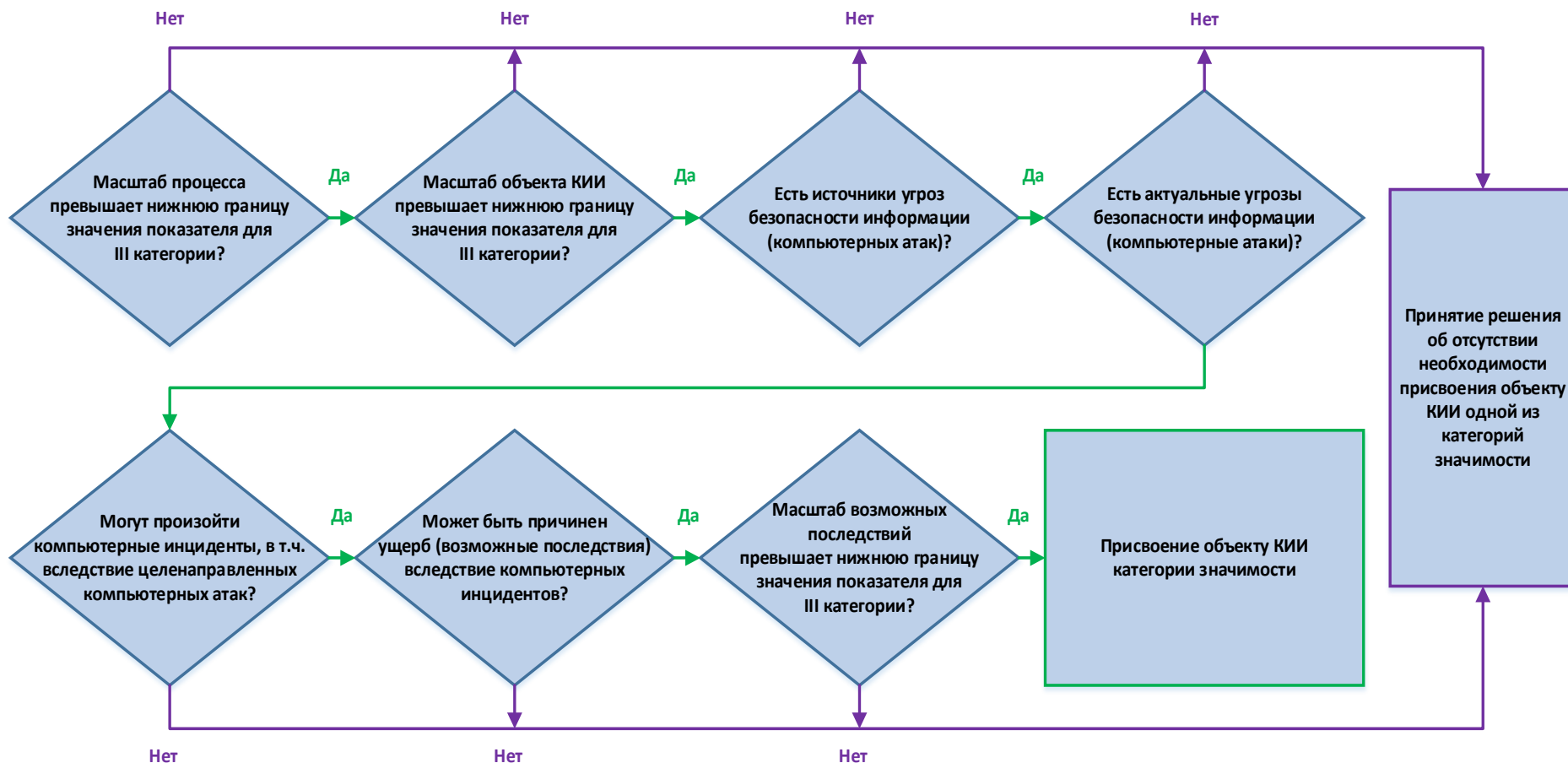
или обоснование их неактуальности

- Оценить в соответствии с перечнем показателей критериев значимости **масштаб возможных последствий в случае возникновения компьютерных инцидентов** на объектах КИИ

или обоснование невозможности наступления компьютерных инцидентов

или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов

От объекта КИИ к решению о значимости



- «Путь» от **сферы деятельности субъекта КИИ** до **перечня объектов КИИ** лежит через анализ процессов
- Используйте стандартизованные подходы по части процессов
- «Путь» от **перечня объектов КИИ** до **принятия решения о значимости** лежит через моделирование угроз
- Используйте методические документы ФСТЭК России (*базовые модели, банк данных угроз bdu.fstec.ru*) и/или «Основные положения базовой модели угроз и нарушителей безопасности информации» (прил. А ГОСТ Р 57580.1-2017)

СПАСИБО ЗА ВНИМАНИЕ!



Кузнецов Александр

Руководитель направления ИБ

+7 (495) 777-13-10

a.kuznetsov@ntc-vulkan.ru

www.ntc-vulkan.ru