Тестовое задание для U Summer Scholl в УЦСБ
Выполнено Меховых Еленой Юрьевной

Проверяемые навыки: 1. Умение работать с актуальным законодательством РФ в сфере ИБ и находить необходимую информацию. 2. Умение систематизировать информацию из разных источников (нормативно-методических документов РФ (НМД), форумов, статей и пр.). 3. Умение анализировать и предлагать варианты выполнения задач (типовых и нетиповых для кандидата). 4. Грамотная письменная речь, соответствующая ожидаемой стилистике, визуализация информации.

Ожидаемый результат: Ответы ожидается в виде документа doc / docx / pdf. При формировании ответов сам текст задания необходимо оставить в неизменном виде, свой ответ писать в отведенном для этого поле. При формировании ответа опирайтесь на нормативные правовые документы, приводите в качестве обоснования своего ответа ссылки на конкретные пункты/статьи законодательных актов. Если для выполнения задания в условиях недостаточно исходных данных - можно делать любые допущения (допущения должны быть прописаны в тексте ответа в явном виде в формате «Предположим, что...»).

Задание №2. ООО «Русская народная компания» занимается производством и поставкой двигателей для военных вертолетов в рамках государственного оборонного заказа, имеет головной офис в г. Екатеринбург (там расположена Администрация) и два производственных филиала в областных городах. Оба филиала являются градообразующими предприятиями, на которых работает около 50% горожан. На текущий момент в компании производилась защита информации отдельных рабочих станций, обрабатывающих государственную тайну, а также в отдельных системах персональных данных (1С: Предприятие и Клиент-банк), иные меры защиты не внедрялись.
Вам, как специалисту по ИБ, поставлены задачи:
1. Определить, попадает ли завод под сферу действия закона о безопасности критической информационной инфраструктуры (КИИ) (является ли субъектом КИИ) и обосновать свою позицию. В случае отнесения к субъектам КИИ, дополнительно указать ответственность для завода в случае, если завод не будет выполнять закон.
2. В случае, если завод относится к субъектам КИИ, подготовить блок-схему, на которой будут представлены основные этапы проведения категорирования объектов КИИ компании. Каждый шаг в блок-схеме необходимо сопроводить ссылкой на норму законодательства: пункт, номер и наименование документа. Если в законодательстве заданы временные ограничения на выполнение тех или иных процедур – их необходимо указать (со ссылкой на норму права). Если в рамках категорирования необходимо оформить документ, форма которого задана нормой законодательства – необходимо это также указать.
3. Определить перечень применимых показателей критериев значимости. Обосновать свое решение (почему показатель применим или неприменим). Показатель считается применимым, если возможен хотя бы какой-то минимальный ущерб (например, если по показателю 1 нарушение процесса приведет к ущербу жизни и здоровью хотя бы одного человека – он применим). Задача не подразумевает расчет значений показателя!
4. Из списка процессов ниже выбрать критические процессы для завода. Предложить и описать методику, по каким критериям и как были оценены процессы.
Перечень процессов завода:
- Инженерное обеспечение завода
- Обеспечение энергоресурсами и поддержание энергооборудования в работоспособном состоянии - Обеспечение работоспособности механического оборудования
- Технологическое обеспечение производства, планирование новых видов продукции
- Разработка и совершенствование технологических процессов - Охрана труда и промышленная безопасность
- Поддержка и развитие заводской корпоративной информационной системы - Метрологическое обеспечение
- Экологический контроль
- Закупка сырья и материалов
- Производство и отгрузка продукции
- Планирование производства и отгрузки продукции
- Организация производства и хранение продукции
- Логистика
- Управление персоналом
- Бухгалтерский учет

Дальнейшие комментарии будут основаны на Федеральном законе "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция) или ссылаясь на другие нормативно-правовые акты (далее - НПА), Федеральные законы (далее - ФЗ) Российской Федерации (далее - РФ). Основной текст задания описан серым цветом, комментарии – черным, желтым цветом выделен ход мыслей.

Задание №2. ООО «Русская народная компания» занимается производством и поставкой двигателей для военных вертолетов в рамках государственного оборонного заказа, имеет головной офис в г. Екатеринбург (там расположена Администрация) и два производственных филиала в областных городах. Оба филиала являются градообразующими предприятиями, на которых работает около 50% горожан. На текущий момент в компании производилась защита информации отдельных рабочих станций, обрабатывающих государственную тайну, а также в отдельных системах персональных данных (1С: Предприятие и Клиент-банк), иные меры защиты не внедрялись.

Вам, как специалисту по ИБ, поставлены задачи:
1. Определить, попадает ли завод под сферу действия закона о безопасности критической информационной инфраструктуры (КИИ) (является ли субъектом КИИ) и обосновать свою позицию. В случае отнесения к субъектам КИИ, дополнительно указать ответственность для завода в случае, если завод не будет выполнять закон.

Примечание 1. Согласно части 8 статье 2 ФЗ-187, субъекты критической информационной инфраструктуры - 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, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.
Примечание 2. Согласно части 7 статье 2 ФЗ-187, объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.
Примечание 3. Согласно части 6 статье 2 ФЗ-187, критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

P.S. ООО "Русская народная компания" (далее - Компания) может рассматриваться как функционирующая в оборонной сфере, исходя из предоставленных сведений, поскольку, по данным материалам, Компания занимается производством и поставкой двигателей для военных вертолетов в рамках государственного оборонного заказа. Факт, что они выполняют заказы в сфере оборонной промышленности, подразумевает, что их деятельность связана с обеспечением оборонных нужд государства. Компании с подобными направлениями деятельности, участвующие в государственном оборонном заказе, работают в оборонной сфере. Они могут производить военное оборудование, оружие, компоненты для военных систем и прочее, что имеет прямое отношение к военной или оборонной деятельности. В данном случае поставка двигателей для военных вертолетов, которые являются частью оборонной инфраструктуры, указывает на то, что Компания занимается производством и поставкой товаров, имеющих применение в оборонной сфере.

Ответственность. Согласно кодексу Российской Федерации об административных правонарушениях (далее – КоАП) от 30.12.2001 N 195-ФЗ (ред. от 28.04.2023), можно выделить ряд административных правонарушений в отношении невыполнения обязанностей соблюдения режима ФЗ-187.
1. Согласно статье 13.12.1 КоАП РФ нарушение требований к созданию систем безопасности значимых объектов КИИ РФ и их эксплуатации влечет наложение штрафа на должностных лиц в размере до пятидесяти тысяч рублей, на юридических лиц – до ста тысяч рублей; нарушение порядка действий при возникновении компьютерных инцидентов влечет наложение штрафа на должностных лиц в размере до пятидесяти тысяч рублей, на юридических лиц – до пятисот тысяч рублей; нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ влечет наложение штрафа на должностных лиц в размере до пятидесяти тысяч рублей, на юридических лиц - до пятисот тысяч рублей.

2. Согласно статье 19.7.15 КоАП РФ Непредставление или нарушение сроков представления сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости ибо представление недостоверных сведений влечет наложение штрафа на должностных лиц в размере до пятидесяти тысяч рублей, на юридических лиц - до ста тысяч рублей; непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ влечет наложение штрафа на должностных лиц в размере до пятидесяти тысяч рублей, на юридических лиц - до пятисот тысяч рублей; повторное совершение административного правонарушения, предусмотренного частью 1 статьи 19.7.15 КоАП РФ влечет наложение штрафа на должностных лиц в размере до ста тысяч рублей, на юридических лиц - до двух тысяч рублей.
Согласно Уголовному кодексу (далее – УК) Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 28.04.2023), можно выделить уголовные правонарушения в отношении невыполнения обязанностей соблюдения режима ФЗ-187.
Согласно статье 274.1 УК РФ, создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ наказывается лишением свободы на срок до пяти лет со штрафом в размере до одного миллиона рублей; неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации , если он повлек причинение вреда КИИ РФ, наказывается лишением свободы на срок до шести лет со штрафом в размере до одного миллиона рублей; Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ или её объектов , если оно повлекло причинение вреда КИИ РФ, наказывается лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового; деяния, предусмотренные частью первой, второй или третьей статьи 274.1 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, наказываются лишением свободы на срок до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового; деяния, предусмотренные частью первой, второй, третьей или четвертой статьи 274.1 УК РФ, если они повлекли тяжкие последствия, наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Примечание 4. Под тяжкими последствиями как квалифицирующим признаком в статьях 272 - 274.1 УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.
В случае, когда подсудимому вменяется признак создания угрозы наступления тяжких последствий, должна быть установлена реальность такой угрозы.

2. В случае, если завод относится к субъектам КИИ, подготовить блок-схему, на которой будут представлены основные этапы проведения категорирования объектов КИИ компании. Каждый шаг в блок-схеме необходимо сопроводить ссылкой на норму законодательства: пункт, номер и наименование документа. Если в законодательстве заданы временные ограничения на выполнение тех или иных процедур – их необходимо указать (со ссылкой на норму права). Если в рамках категорирования необходимо оформить документ, форма которого задана нормой законодательства – необходимо это также указать.

P.S. Блок схема оформлена согласно ГОСТ 19.701-90 (ИСО 5807-85)1 и представлена на рисунке 1. Блок-схема была составлена согласно НПА таким, как Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", постановление Правительства РФ от 08.02.2018 N 127 (ред. от 20.12.2022) "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации (далее – ПП РФ №127), Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. n 236 "Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий" (далее – Приказ ФСТЭК №236).

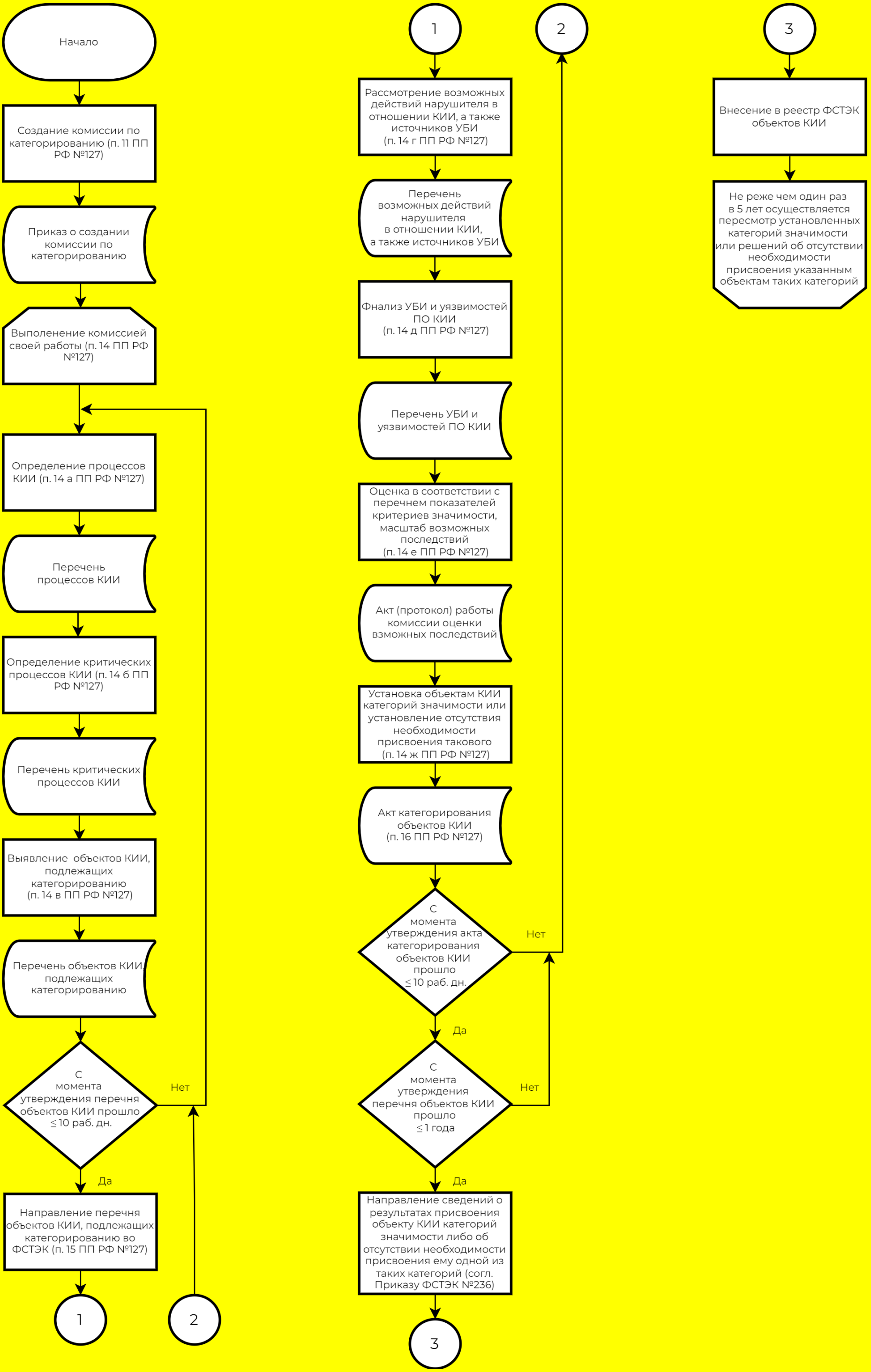

Рисунок 1 – Блок схема основных этапов проведения категорирования объектов КИИ компании

3. Определить перечень применимых показателей критериев значимости. Обосновать свое решение (почему показатель применим или неприменим). Показатель считается применимым, если возможен хотя бы какой-то минимальный ущерб (например, если по показателю 1 нарушение процесса приведет к ущербу жизни и здоровью хотя бы одного человека – он применим). Задача не подразумевает расчет значений показателя!

P.S. Определение перечня применимых показателей критериев значимости далее производится согласно п. 4 ПП №127 перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (далее - Перечень), утвержденным ПП РФ №127.

По данным, определенным ранее, Компания может рассматриваться как функционирующая в оборонной сфере, следовательно, согласно части V Перечня необходимо рассматривать значения показателей для обеспечения обороны страны, безопасности государства и правопорядка. По представленным показателям критериев значимости части V Перечня, можно выделить пункт 13 «Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры», что соответствует применимому показателю критериев значимости.

4. Из списка процессов ниже выбрать критические процессы для завода. Предложить и описать методику, по каким критериям и как были оценены процессы.

Перечень процессов завода:
- Инженерное обеспечение завода
- Обеспечение энергоресурсами и поддержание энергооборудования в работоспособном состоянии - Обеспечение работоспособности механического оборудования
- Технологическое обеспечение производства, планирование новых видов продукции
- Разработка и совершенствование технологических процессов - Охрана труда и промышленная безопасность
- Поддержка и развитие заводской корпоративной информационной системы - Метрологическое обеспечение
- Экологический контроль
- Закупка сырья и материалов
- Производство и отгрузка продукции
- Планирование производства и отгрузки продукции
- Организация производства и хранение продукции
- Логистика
- Управление персоналом
- Бухгалтерский учет

P.S. В связи с отсутствием конкретных методов определения критических процессов в действующем законодательстве РФ о КИИ. Выделю следующую методику. Критическими следует считать те процессы, нарушение которых может иметь негативные последствия, согласно в Перечню. Таким образом, будет определена конкретная группа объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения нормального функционирования этих критических процессов.
Перечень критических процессов Компании и их оценка представлены в таблице 1.

Таблица 1

Перечень критических процессов Компании

№	Критический процесс	Критерий	Оценка
1	Инженерное обеспечение завода	Нарушение вызовет негативные последствия, согласно части V Перечня	Критический
2	Обеспечение энергоресурсами и поддержание энергооборудования в работоспособном состоянии - Обеспечение работоспособности механического оборудования	Нарушение вызовет негативные последствия, согласно части V Перечня	Критический
3	Технологическое обеспечение производства, планирование новых видов продукции	Нарушение вызовет негативные последствия, согласно части V Перечня	Критический
4	Разработка и совершенствование технологических процессов - Охрана труда и промышленная безопасность	Нарушение вызовет негативные последствия, согласно части V Перечня	Критический
5	Поддержка и развитие заводской корпоративной информационной системы - Метрологическое обеспечение	Нарушение вызовет негативные последствия, согласно части V Перечня	Критический

Продолжение таблицы 1

6	**Экологический контроль**	**Нарушение не вызовет негативные последствия, согласно части V Перечня**	**Некритический**
7	**Закупка сырья и материалов**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
8	**Производство и отгрузка продукции**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
9	**Планирование производства и отгрузки продукции**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
10	**Организация производства и хранение продукции**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
11	**Логистика**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
12	**Управление персоналом**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**
13	**Бухгалтерский учет**	**Нарушение вызовет негативные последствия, согласно части V Перечня**	**Критический**

Из таблицы следует что, критическими процессами можно выделить все представленные, кроме процесса «Экологический контроль», поскольку ни на один из показателей критериев значимости части V Перечня нарушение данного процесса не повлияет.

---

[1] ГОСТ 19.701-90 (ИСО 5807-85) – URL: https://clck.ru/34Qrp2 (Дата обращения: 15.05.2023)