НПП “Гамма”

Практический опыт реализации требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» на предприятиях промышленности

Докладчик: Григорян Степан
Тел.: 8 932 120 99 25
e-mail: stgrigoryan@gammaural.ru

2021 г.

НПП "Гамма"

Особенности проведения процедуры категорирования объектов КИИ на предприятии

Целесообразность создания обособленной системы мониторинга событий информационной безопасности при взаимодействии с ГосСОПКА

Практический опыт ФГУП "НПП "Гамма"

НПП “Гамма”

Перечень работ	Аудит информационной безопасности предприятий
	Подготовка сведений для категорирования объектов КИИ
	Разработка (проектирование) систем безопасности ЗОКИИ
	Внедрение и приемочные испытания систем безопасности ЗОКИИ
	Сопровождение систем безопасности ЗОКИИ в ходе их эксплуатации
	Мониторинг событий информационной безопасности
	Внешний аудит систем безопасности ЗОКИИ
	Разработка и построение систем мониторинга событий информационной безопасности

Практический опыт ФГУП "НПП "Гамма"

НПП "Гамма"

Энергетика

- Нижневартовская ГРЭС
- Кемеровская ГРЭС
- Красноярская ТЭЦ
- СТСК
- СаровГаз
- СЭСК
- СГК
- Обеспечение РФЯЦ-ВНИИЭФ

Область атомной энергии

- АО ЧМЗ

Оборонная промышленность

- ППЗ
- КумАПП
- Уралкриомаш
- 144 БТРЗ
- ХЗ Планта
- НИИЭП
- Златмаш
- Уралвагонзавод
- УОМЗ

Ракетно-космическая промышленность

- НПО электромеханики
- УПКБ Деталь
- Искра
- РКЦ Прогресс
- Протон-ПМ

Горнодобывающая и металлургическая промышленность

- УГМ
- НМЗ
- КМЭЗ
- Карабашмедь
- ЕЗ ОЦМ
- БСЗ
- БСК

Связь

- МТС

НПП "Гамма"

Объект и субъект

Объект КИИ – ИС, ИТКС, АСУ субъектов КИИ.

Субъект КИИ – госорганы, госучреждения, российские ЮЛ и (или) ИП, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, 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 ЮЛ и (или) ИП, которые обеспечивают взаимодействие указанных систем или сетей.

Основные понятия

НПП "Гамма"

Типы объектов

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 (ФЗ 187).

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (ФЗ 149).

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (ФЗ 149).

Основные понятия

НПП “Гамма”

Ответственность (ФЗ 194)	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия (от двух до пяти лет).
	Неправомерный доступ к охраняемой компьютерной информации (от двух до шести лет).
	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации (до шести лет).
	Те же деяния, совершенные группой лиц по предварительному сговору (от трех до восьми лет).
	Те же деяния, повлекшие тяжки последствия (от пяти до десяти лет).

Особенности проведения процедуры категорирования объектов КИИ на предприятии

НПП “Гамма”

Отнесение предприятия к числу субъектов КИИ

Отнесение ИС, ИТКС, АСУ к объектам КИИ

Процессы / критические процессы,

Определение актуальных критериев значимости для предприятия

Угрозы безопасности информации

Масштаб возможных последствий в случае возникновения компьютерных инцидентов

Формирование перечня ИС, ИТКС, АСУ

НПП “Гамма”

Определение необходимости отнесения предприятия к числу субъектов КИИ

- Устав
- Коды ОКВЭД
- Лицензии

Формирование перечня объектов КИИ

- ИС
- ИТКС
- АСУ

Формирование перечня ИС, ИТКС, АСУ

НПП "Гамма"

Пример перечня ИС, ИТКС, АСУ

№ п/п	Название объекта	Назначение объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект
1	АСУТП производства соляной кислоты	Контроль и управление процессом производства соляной кислоты	АСУ	Химическая пром-ть
2	АСУТП производства пара и электрической энергии	Контроль и управление процессом производства пара и электрической энергии для нужд предприятия	АСУ	Энергетика
3	ЛВС предприятия	Обеспечение функционирования информационной инфраструктуры предприятия	ИТКС	Химическая пром-ть
4	1С: Предприятие	Автоматизация процессов бухгалтерского и налогового учета, формирования документов (финансовых, отгрузочных)	ИС	Химическая пром-ть
5	СКУД	Обеспечение автоматизированного пропуска работников и посетителей на территорию предприятия	АСУ	*Отсутствует*

Определение бизнес-процессов

НПП "Гамма"

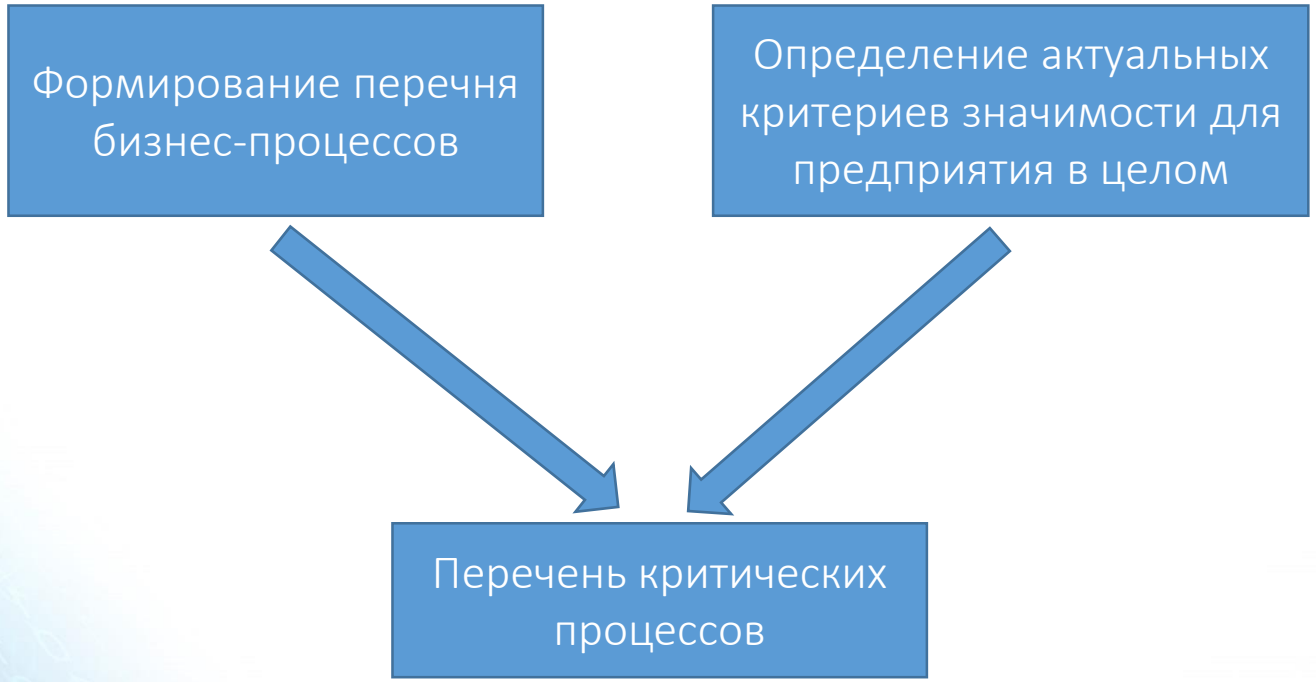
Процессы	Управленческие
	Технологические
	Производственные
	Финансово-экономические
	Иные

№ п/п	Наименование процесса	Принадлежность процесса к сферам деятельности
1	Процесс 1	Сфера 1
2	Процесс 2	Сфера 2
…	…	…
N	Процесс N	Сфера 1

Определение критических процессов

НПП “Гамма”

Критический процесс – бизнес-процесс, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.



Определение актуальных критериев значимости для предприятия в целом

НПП “Гамма”

Исключение блоков критериев

- *политическая значимость*
- *экологическая значимость*

Исключение конкретных показателей

- *показатель 3 (транспортная инфраструктура);*
- *показатель 10 (операции по банковским счетам);*
- *показатель 12 (ситуационный центр).*

Определение критических процессов

НПП "Гамма"

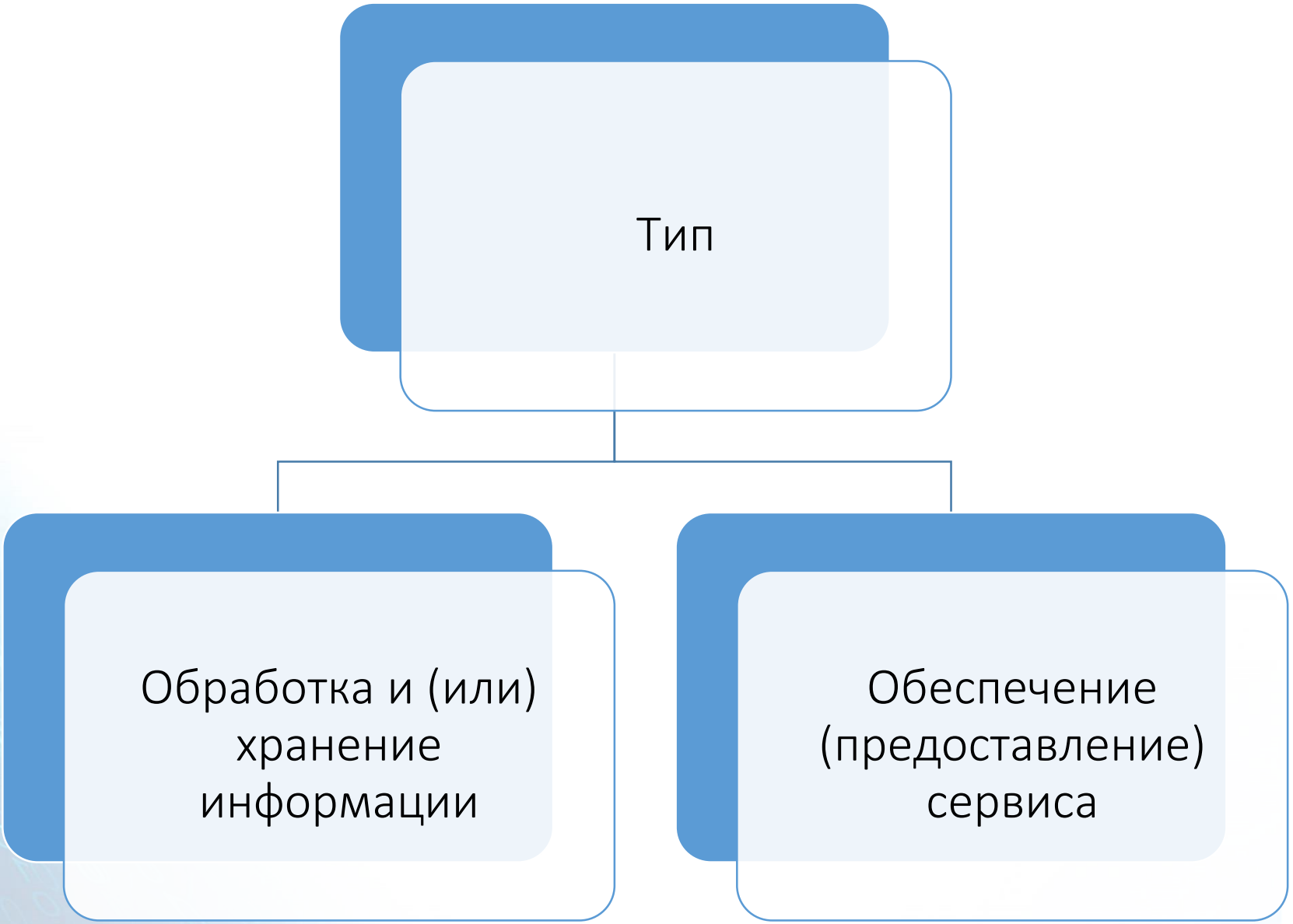
№ п/п	Наименование процесса	Принадлежность процесса к сферам деятельности	Показатели потенциального влияния процесса на деятельность Общества в соответствии с показателями критериев значимости объектов КИИ Российской Федерации, утвержденных ПП № 127		
			п. 1 раздела I Перечня ПКЗ	п. 9 раздела III Перечня ПКЗ	п. 11 раздела IV Перечня ПКЗ
1	Процесс 1	Сфера 1	Да	Нет	Да
2	Процесс 2	Сфера 1	Нет	Да	Нет
3	Процесс 3	Сфера 2	Нет	Нет	Нет

Определение информации, необходимой для обеспечения критических процессов

НПП "Гамма"

Определение объектов КИИ, подлежащих категорированию

НПП “Гамма”



Определение объектов КИИ, подлежащих категорированию

НПП "Гамма"

№ п/п	Наименование критического процесса	Наименование объекта КИИ	Оценка потенциального влияния объекта КИИ на КП	Описание влияния объекта КИИ на КП
1	Процесс 1	**Объект 1**	Да	Осуществляет управление и контроль критического процесса
2	Процесс 1	**Объект 2**	Да	Осуществляет обработку и хранение информации, необходимой для обеспечения критического процесса
3	Процесс 2	Объект 3	Нет	*Отсутствует*
4	Процесс …	…	…	…
5	Процесс N	**Объект Т**	Да	Осуществляет мониторинг критического процесса

Формирование перечня объектов КИИ, подлежащих категорированию

НПП “Гамма”

ИС от 17 апреля 2020 г. № 240/84/611

Рекомендуемая форма перечня объектов.

Порядок передачи (бумажный и электронный вид).

Формат направляемых файлов (ods/odt).

Сроки предоставления сведений

Вопросы

НПП "Гамма"

Проблема	Решение
Неактуальные коды ОКВЭД	Актуализация кодов
Формализация бизнес-процессов	Система менеджмента качества/ разработка перечня процессов
Перечень ИС, ИТКС, АСУ	Проведение детального аудита предприятия
Уровень конфиденциальности	Сверка с перечнями сведений
Важность систем	Стресс-тесты
Контроль изменений	Периодическая актуализация перечней (процессов, объектов, информации) / аудит текущего состояния

Особенности проведения процедуры категорирования объектов КИИ на предприятии

НПП “Гамма”

Проблематика	Сложность и (или) отсутствие возможности изменения архитектуры
	Устаревание элементов
	Отсутствие возможности создания показательного тестового стенда
	Отсутствие средств восстановления
	Наличие локального доступа сторонних организаций
	Наличие постоянного удаленного доступа
	Отсутствие мониторинга состояния информационной безопасности

Целесообразность создания обособленной системы мониторинга событий информационной безопасности при взаимодействии с ГосСОПКА

НПП "Гамма"

Мониторинг состояния ИБ

НПП “Гамма”

Спасибо за внимание!

Докладчик: Григорян Степан
Тел.: 8 932 120 99 25
e-mail: stgrigoryan@gammaural.ru