ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Подключение КИИ к ГосСОПКА

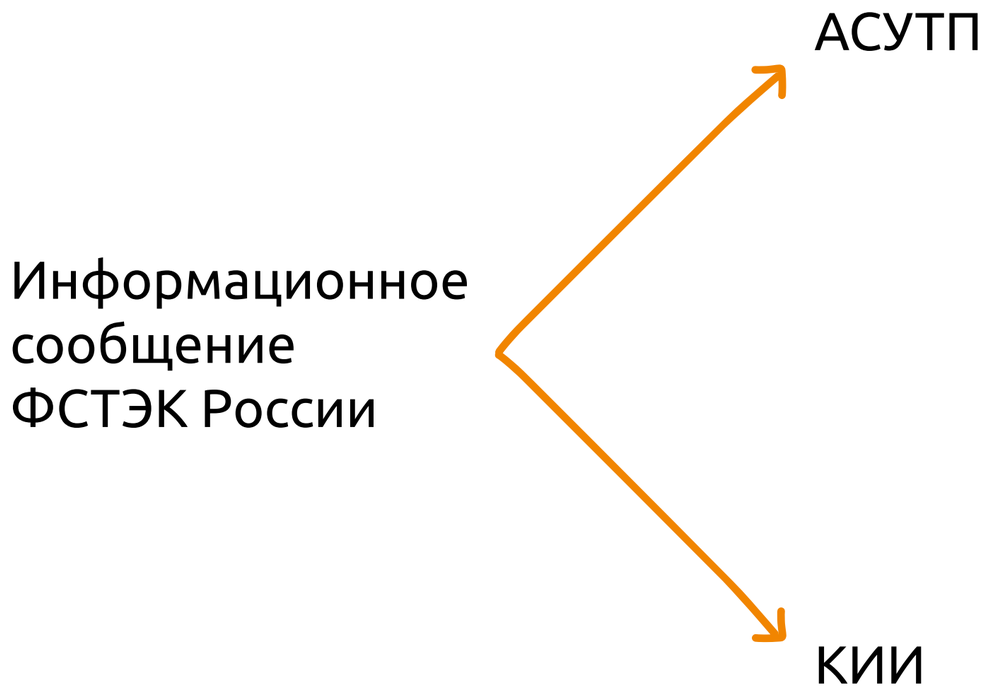
Артём Савчук

Заместитель технического директора
компании «Перспективный мониторинг»

Предыстория = КСИИ

Для обеспечения безопасности информации в КСИИ, в ФСТЭК России была разработана и утверждена система методических документов (ДСП, 2007 г.)

С выходом новых документов по защите АСУТП и КИИ старые документы по защите КСИИ можно применять с некоторыми ограничениями:



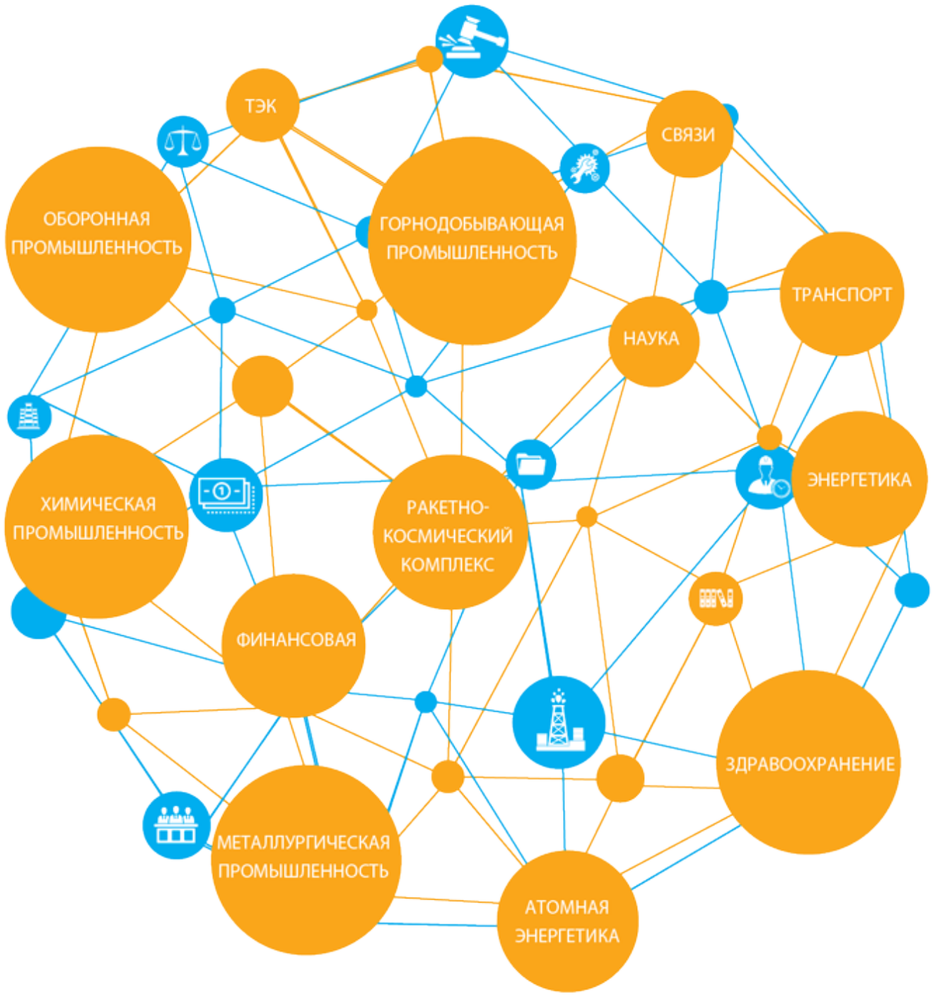
Что такое КИИ?

Согласно закону № 187-ФЗ, КИИ:

> информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

Подмножеством всех объектов КИИ являются **значимые объекты КИИ.**

К субъектам КИИ относятся владельцы объектов КИИ, а также организации, которые обеспечивают их взаимодействие.



Нормативные документы в области ГосСОПКА и безопасности КИИ

Федеральные законы:

1) ФЗ от 26.07.2017 № 187-ФЗ *«О безопасности КИИ РФ»*

2) ФЗ от 26.07.2017 № 194-ФЗ *«О внесении изменений в УК РФ и статью 151 Уголовно-процессуального кодекса РФ в связи с принятием ФЗ "О безопасности КИИ РФ"»*

3) ФЗ от 26.07.2017 № 193-ФЗ *«О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ " О безопасности КИИ РФ "»*

Акты Президента РФ:

1) Указ Президента РФ от 25.11.2017 № 569 *«О внесении изменений в Положение о ФСТЭК...»*

2) Указ Президента РФ от 02.03.2018 № 98 *«О внесении изменения в перечень сведений, отнесённых к гостайне...»*

3) **Указ Президента РФ от 01.05.2022 № 250 *«О дополнительных мерах по обеспечению информационной безопасности РФ»***

Нормативные документы в области ГосСОПКА и безопасности КИИ

Акты Правительства РФ:

1) ПП РФ от 08.02.2018 № 127 *«Об утверждении Правил категорирования ОКИИ РФ, а также перечня показателей критериев значимости ОКИИ РФ и их значений»*

2) ПП РФ от 17.02.2018 № 162 *«Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых ОКИИ РФ»*

3) **ПП РФ от 8.06.2019 № 743** ***«Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых ОКИИ»***

Нормативные документы в области ГосСОПКА и безопасности КИИ

Ведомственные акты [Приказы ФСТЭК России]:

1) от 06.12.2017 № 227 *«Об утверждении Порядка ведения реестра ЗОКИИ РФ»*

2) от 11.12.2017 № 229 *«Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности ЗОКИИ РФ»*

3) от 21.12.2017 № 235 *«Об утверждении Требований к созданию систем безопасности ЗОКИИ РФ и обеспечению их функционирования»*

4) от 22.12.2017 № 236 «*Об утверждении формы направления сведений о результатах присвоения ОКИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»*

5) от 25.12.2017 № 239 *«Об утверждении Требований по обеспечению безопасности ЗОКИИ РФ»*

6) от 26.04.2018 № 72 *«О внесении изменений в Регламент ФСТЭК, утвержденный приказом ФСТЭК России от 12 мая 2005 г. № 167»*

7) от 09.08.2018 № 138 «*О внесении изменений в Требования к обеспечению ЗИ в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах…»*

Нормативные документы в области ГосСОПКА и безопасности КИИ

Информационное сообщение:

ФСТЭК России от 24.08.2018 № 240/25/3752 по *вопросам представления перечней ОКИИ, подлежащих категорированию*, и направления сведений о результатах присвоения ОКИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Безопасность ЗОКИИ

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 *«Об утверждении Требований по обеспечению безопасности ЗОКИИ РФ».*

Требования к СВТ и СЗИ, применяемым для защиты значимого объекта КИИ			
Категория значимости объекта КИИ	Класс средств вычисли-тельной техники	Уровень контроля отсутствия НДВ	Класс защиты СЗИ
1 категория	Не ниже 5 класса	Не ниже 4 уровня	Не ниже 4 класса
2 категория	Не ниже 5 класса	Не ниже 4 уровня	Не ниже 5 класса
3 категория	Не ниже 5 класса	—	Не ниже 6 класса

В случае, если ОКИИ является ГосИС, то применяются нормы Приказа ФСТЭК России №17 по защите ГИС и проводится его аттестация.

Критерии отнесения объектов КИИ к значимым описаны в ПП №127.

Кроме значимых объектов, по решению СКИИ нормы рассматриваемого документа могут применяться и к незначимым объектам, равно как и требования Приказа №31.

В Приказе №239 отдельно указано, что ОКИИ, обрабатывающие ПДн, попадают также и под нормы защиты ПДн.

АСУТП

Приказ ФСТЭК России от 14 марта 2014 г. № 31 в ред. Приказа ФСТЭК России от 9 августа 2018 г. № 138 устанавливает законодательные требования в области обеспечения безопасности АСУТП.

Несмотря на наличие 187-ФЗ с подзаконными актами и Приказа №31, в настоящее время государственные регуляторы придерживаются следующей точки зрения:

Если ОКИИ признан значимым, то

используется Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности ЗОКИИ РФ»

Если ОКИИ признан незначимым, то

по решению СКИИ можно применять как Приказ №31 по АСУТП, так и Приказ №239 по КИИ.

Что такое ГосСОПКА?

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на ИР РФ.

НКЦКИ организует сбор и обмен информацией об инцидентах между СКИИ, координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению КА.

В соответствии с разработанным в ФСБ РФ документом №149/2/7-200 от 24 декабря 2016 г. *«Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий КА на ИР РФ».*

Функции ГосСОПКА

Класс В	Класс Б	Класс А
Взаимодействие с НКЦКИ	Анализ угроз ИБ, прогнозирование их развития и направление в НКЦКИ результатов	Ликвидация последствий компьютерных инцидентов
Разработка регламентирующих документов	Формирование предложений по повышению уровня защищённости информационных ресурсов	Анализ результатов ликвидации последствий инцидентов
Эксплуатация средств ГосСОПКА	Выявление уязвимостей информационных ресурсов	
Приём сообщений об инцидентах от персонала и пользователей информационных ресурсов	Составление перечня инцидентов	
Приём сообщений об инцидентах от персонала и пользователей информационных ресурсов	Установление причин компьютерных инцидентов	
Анализ событий ИБ	Составление и актуализация перечня угроз ИБ	
Инвентаризация информационных ресурсов		

Механизм работы ГосСОПКА

Информация по произошедшему компьютерному инциденту должна быть передана СКИИ в систему ГосСОПКА в объёме, согласно положениям Приказа ФСБ РФ № 367, с момента обнаружения компьютерного инцидента:

- **Не позднее 24 часов для НОКИИ**
- **Не позднее 3 часов для ЗОКИИ**

Способы подключения к НКЦКИ:

- ViPNet
- Континет
- С-Терра Шлюз
- Центр ГосСОПКА

Корпоративный Центр АО «Перспектиивный мониторинг» является центром системы ГосСОПКА класса А с 2017 года.

НПА в сфере ГосСОПКА

Акты Президента РФ:

1) Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (Утверждены 03.02.2012 г. № 803)

2) Указ Президента РФ от 15.01.2013 № 31с *«О создании ГосСОПКА на ИР РФ»*

3) Концепция ГосСОПКА на ИР РФ, утверждённая Президентом РФ 12 декабря 2014 г. № К 1274

4) План развёртывания ведомственных сегментов ГосСОПКА, утвержденный Президентом РФ 21 августа 2015 г., № 9397

5) Указ Президента РФ от 22.12.2017 № 620 *«О совершенствовании ГосСОПКА на ИР РФ»*

НПА в сфере ГосСОПКА

Ведомственные акты [Приказ ФСБ России]:

1) от 24.07.2018 № 366 *«О Национальном координационном центре по КИ»*

2) от 24.07.2018 № 367 *«Об утверждении Перечня информации, представляемой в ГосСОПКА на ИР РФ и Порядка представления информации...»*

3) от 24.07.2018 № 368 *«Об утверждении Порядка обмена информацией о КИ между СКИИ РФ...»*

4) от 06.05.2019 № 196 *«Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ»*

5) от 19.06.2019 № 281 *«Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ...»*

6) от 19.06.2019 № 282 *«Об утверждении Порядка информирования ФСБ России о КИ, реагирования на них, принятия мер по ликвидации последствий КА...»*

7) Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА на ИР РФ от 27.12.2016

Полномочия

ФСТЭК России

назначен федеральным органом исполнительной власти, **уполномоченным в области обеспечения безопасности КИИ РФ.**

ФСБ РФ

возложены функции федерального органа исполнительной власти, уполномоченного в области **обеспечения функционирования ГосСОПКА на ИР РФ.**

В ведении ФСБ РФ находится НКЦКИ. НКЦКИ координирует деятельность СКИИ и является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, а техническая инфраструктура НКЦКИ используется для функционирования системы ГосСОПКА.

Обязанности субъектов КИИ

КИИ

- информировать НКЦКИ об инцидентах
- содействовать НКЦКИ в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения инцидентов
- обеспечивать выполнение порядка, технических условий установки и эксплуатации, сохранность средств ГосСОПКА (если они установлены на объектах КИИ)

ЗОКИИ

- создать систему безопасности ЗОКИИ и обеспечить её функционирование

Основные задачи системы безопасности:

1) предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения информации, обрабатываемой ЗОКИИ
2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ЗОКИИ...

Обязанности субъектов КИИ

КИИ

- информировать НКЦКИ об инцидентах
- содействовать НКЦКИ в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения инцидентов
- обеспечивать выполнение порядка, технических условий установки и эксплуатации, сохранность средств ГосСОПКА (если они установлены на объектах КИИ)

ЗОКИИ

3) восстановление функционирования ЗОКИИ, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации

4) **непрерывное взаимодействие с ГосСОПКА**

- выполнять предписания ФСТЭК об устранении нарушений ИБ ЗОКИИ
- обеспечивать доступ ФСТЭК к ЗОКИИ при проверках
- **реагировать на инциденты, принимать меры по ликвидации последствий**

Что подразумевается под интеграцией с ГосСОПКА?

Интеграция в ГосСОПКА требует от СКИИ:

- установить двухсторонние рабочие и договорные отношения с НКЦКИ
- информировать о КИ НКЦКИ, а также ЦБ РФ, если организация осуществляет деятельность в банковской сфере и иных сферах финансового рынка
- оказывать содействие НКЦКИ в обнаружении, предупреждении и ликвидации последствий КА, установлении причин и условий возникновения КИ

Кроме того, по решению СКИИ на территории ОКИИ может быть размещено оборудование ГосСОПКА.

В этом случае субъект дополнительно обеспечивает его сохранность и бесперебойную работу. Также СКИИ может создать собственный центр ГосСОПКА.

Варианты исполнения

Самостоятельно

- Провести категорирование
- Обеспечить информационный обмен с НКЦКИ
- Выполнить организационные и технические требования в соответствии с НПА и методическими рекомендациями
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ (для ЗОКИИ)

Силы, средства, документы, процессы, ответственность

Через корпоративный центр ГосСОПКА

- Заключить договор с корпоративным центром
- Уведомить НКЦКИ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ГОССОПКА

₽ ₽ ₽

Условия подключения к ГосСОПКА

1. Субъекты КИИ

- По требованиям закона [п.1 ч.2 ст.9 ФЗ-187]

2. Организации-лицензиаты, для оказания услуг

3. Организации для собственных нужд

В соответствии с законом [ч.5 ст.5 ФЗ-187] к ГосСОПКА могут подключаться иные организации.

Необходимо стать субъектом ГосСОПКА:

- выполнить требования для центров ГосСОПКА
- заключить соглашение с ФСБ России

Условия для создания центра ГосСОПКА

1. Получить лицензии

- ФСБ России на право осуществления работ, связанных с использованием сведений, составляющих гостайну (в случае если обрабатывается ГТ)
- ФСТЭК России на деятельность по ТЗКИ (по части мониторинга)
- Одну из лицензий ФСБ России на право:

1) осуществления работ, связанных с созданием СЗИ, содержащей сведения, составляющие гостайну;

2) деятельности, связанной с шифровальными средствами.

2. Разработать документы

- Положение о центре ГосСОПКА
- Регламент деятельности центра
- Штатное расписание центра

3. Заключить соглашение

- О взаимодействии с ФСБ России в области обнаружения, предупреждения и ликвидации последствий атак

Преимущества КЦ ГосСОПКА as Service

- Оптимизация затрат на ИБ за счёт сервисной модели
- Высокий уровень устойчивости к киберугрозам
- Быстрый старт и масштабируемость
- Качественный сервис вместо длительного интеграционного проекта

Ст. 10 187-ФЗ «системы безопасности ЗОКИИ должны обеспечивать непрерывное взаимодействие с ГосСОПКА.

Подключение к внешнему (коммерческому) центру ГосСОПКА позволяет передать задачи в области обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ специализированной организации.

- Кроме того, воспользовавшись услугами внешнего центра ГосСОПКА, организация перекладывает на исполнителя риски несоответствия законодательству РФ в области ведения незаконного предпринимательства (ст. 171 УК РФ) в части ведения деятельности без соответствующих лицензий ФСБ РФ и/или ФСТЭК России.

Уголовная ответственность

За неправомерное воздействие на КИИ РФ предусмотрена статьей 274.1 УК РФ.
Данная статья была введена ФЗ № 194 от 26.07.2017 г. и действует с 01.01.2018 г.
В соответствии с данной статьей уголовно наказуемы:

1. создание, распространение и использование программ для неправомерного воздействия на КИИ;

2. неправомерный доступ к информации в КИИ с последовавшим причинением вреда КИИ

3. нарушение правил эксплуатации средств хранения, обработки, передачи информации в КИИ или правил доступа к информации в КИИ с последовавшим причинением вреда КИИ

4. указанные выше действия, совершенные группой лиц по предварительному сговору, или в составе организованной группы, или с использованием служебного положения

5. указанные выше действия, если они повлекли тяжкие последствия (т.е. причинен ущерб на сумму более 1 миллиона рублей), при этом наступает ответственность в виде лишения свободы на срок до десяти лет, что автоматически переводит данное деяние в разряд тяжких преступлений со сроком давности до 10 лет.

Административная ответственность

Также приняты изменения в КоАП РФ:

Статья 13.12.1

«Нарушение требований в области обеспечения безопасности КИИ РФ» предусматривает ответственность за нарушение порядка категорирования ОКИИ, нарушение требований к созданию и обеспечению функционирования систем безопасности ЗОКИИ, нарушение требований по обеспечению безопасности ЗОКИИ, а также нарушение порядка информирования, реагирования и обмена информацией о КИ

Статья 19.7.15

«Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности КИИ РФ» предполагает ответственность за нарушение порядка предоставления сведений о категорировании объектов КИИ во ФСТЭК России, а также за невыполнение норм по обмену информацией с ГосСОПКА.

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Артём Савчук

Заместитель технического
директора компании
«Перспективный мониторинг»

Artem.Savchuk@amonitoring.ru

t.me/pm_public

amonitoring.ru

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Категорирование объектов КИИ

Взаимодействие подразделений, кто должен принимать участие

Сергей Петров

Старший аналитик обособленного подразделения
«Перспективный мониторинг» в г. Пенза

Указ Президента РФ
от 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности РФ»

- Федеральные и государственные органы исполнительной власти
- Государственные фонды и компании
- Стратегические предприятия и АО
- Организации системообразующие и созданные на основании федеральных законов
- Юридические лица, являющиеся субъектами КИИ

Постановление Правительства РФ № 127

Состав Комиссии по категорированию:

- Руководитель субъекта КИИ или уполномоченное им лицо
- Специалисты в области выполняемых функций, ИТ и связи, а также по эксплуатации тех. оборудования, безопасности, контролю и учёту опасных веществ и материалов
- Работники подразделений ИБ, защиты гос. тайны и структурного подразделения ГО
- Могут быть включены другие работники, в т.ч. финансово-экономического подразделения

В чём проблема?

- Ты ИБэшник. Сам с этим и разбирайся
- Комиссию создадим на бумаге, но будешь делать сам
- Данные дам, но в комиссию не пойду. Не моя зона ответственности
- Какие данные для вашей безопасности… мне некогда вашей ерундой заниматься
- Я в оценке КИИ ничего не понимаю, зачем меня включать в комиссию
- Пригласите внешнюю организацию и пусть за нас сделают

Кого включать в Комиссию
и в какой форме?

Комиссия *на постоянной основе*

1) Понимание того, как устроена деятельность организации
2) Организация сбора информации и проведения расчётов
3) Валидация предоставленной информации
4) Проверка расчётов
5) Принятие итоговых решений по результатам

Другие специалисты *на временной основе*

1) Сбор информации
2) Проведение расчётов
3) Оформление результатов

Когда нужна информация для категорирования объектов КИИ?

Для определения:

- Сфер / видов деятельности организации как субъекта КИИ
- Перечня процессов и выделения критических процессов организации
- Перечня объектов КИИ организации, подлежащих категорированию
- Актуальных угроз безопасности информации
- Для оценки масштаба возможных негативных последствий от нарушения / прекращения функционирования объектов КИИ
- Для оформления результатов категорирования объектов КИИ и подготовки документов для ФСТЭК России

Определение сфер / видов деятельности организации как субъекта КИИ

Информация	Источник
Устав Выписка из Единого государственного реестра юрлиц Лицензии Сертификаты	Администрация Делопроизводство Руководитель
Законодательство РФ: • о защите населения и территорий от ЧС природного и техногенного характера; • о промышленной безопасности опасных производств; • об охране окружающей среды; • о транспортной безопасности; • об организации предоставления гос. и муниципальных услуг; • о международных договорах РФ; • о некоммерч. орг. (гос. корпорации и компании);	Юридическая служба

Определение сфер / видов деятельности организации как субъекта КИИ

Информация	Источник
• о гос. и муниципальных унитарных предприятиях; • стратегические акционерные общества; • о банках и банковской деятельности; • о методике определения СЗКО; • об установлении значений критериев СЗПС; • о признании ИОФР системно значимыми;	Юридическая служба
Виды деятельности выделены и структурированы Процессная документация	Методологическое подразделение
Виды деятельности **не выделены** и **не структурированы** Сведения об организационно-штатной структуре	Кадровая служба Представители структурных подразделений
Договоры с другими субъектами КИИ	Договорной отдел Бухгалтерский и налоговый учёт

Определение перечня процессов и выделение критических процессов организации

Информация	Источник
Процессы определены и описаны *(основные, управленческие, обеспечивающие).* Процессная документация	Методологическое подразделение
Процессы **не определены** Сведения об организационно-штатной структуре Положения различных подразделений	Кадровая служба Представители структурных подразделений
Перечень критических процессов *(результаты оценки рисков)*	Подразделение риск-менеджмента Представители структурных подразделений

Определение перечня объектов КИИ организации, подлежащих категорированию

Информация	Источник
Перечень АС, ИС, ИТКС, АСУ	ИТ-подразделение
Договоры: • на приобретение систем • на разработку систем • на обслуживание промышленного оборудования, и т.п.	Договорной отдел Бухгалтерский и налоговый учёт
Системы управления: • критически важными и потенциально опасными объектами • опасными производственными объектами • объектами, оказывающими негативное возд. на окр. среду	Представители структурных подразделений

Определение актуальных угроз безопасности информации

Негативные последствия угроз безопасности информации

- Подразделение риск-менеджмента
- Представители структурных подразделений

Способы реализации угроз безопасности информации

- ИТ-подразделение
- Служба ИБ

Оценка актуальности угроз безопасности информации

- ИТ-подразделение
- Служба ИБ

Объекты воздействия угроз безопасности информации

- ИТ-подразделение

Источники угроз безопасности информации

- Служба ИБ

Оценка масштаба возможных негативных последствий от нарушения / прекраще-ния функционирования объектов КИ

Информация	Источник
Характеристики основной деятельности организации: • регионы присутствия / оказания услуг • масштабы территории (район, город, область и т.п.) • кол-во пользователей / абонентов услуг (транспорт, водоснабжение, связь, медицина, электричество и т.п.) • количество банковских операций • государственные услуги • ситуационный центр • государственный оборонный заказ • показатели эффективности деятельности и т.д.	Представители структурных подразделений Финансово-экономическое подразделение Подразделения статистики Аналитические подразделения Внутренний контроль

Оценка масштаба возможных негативных последствий от нарушения / прекраще-ния функционирования объектов КИ

Информация	Источник
Характеристики опасных видов деятельности: • данные о численности населения • число человек в зоне потенциальной опасности • паспорт безопасности опасного объекта • план действий по предупреждению и ликвидации ЧС	Подразделение по ГОиЧС Подразделение оп охране окружающей среды
Договорные отношения: • договоры с гос. органами / корпорациями / предприятиями • международные договоры • договоры с другими субъектами КИИ и т.д.	Договорной отдел Бухгалтерский и налоговый учёт

Оценка масштаба возможных негативных последствий от нарушения / прекраще-ния функционирования объектов КИ

Информация	Источник
Экономические характеристики: • налоги и сборы (на прибыль, добычу ископаемых, дивиденды) • прибыль организации • различные виды затрат на ликвидацию и восстановление (возмещ. вреда, ликвидация аварии, восстановление производства, материальные потери, оплата труда, срыв контрактов и т.п.)	Финансово-экономическое подразделение Бухгалтерский и налоговый учёт
Характеристики непрерывности объектов ИТ: • допустимое время простаивания АС • фактическое время простаивания АС • время восстановления по SLA	ИТ-подразделение
Результаты оценки операционных рисков от нарушения функционирования ИТ-инфраструктуры	Подразделение риск-менеджмента

Оформление результатов категорирования объектов КИИ и подготовка документов для ФСТЭК России

Информация	Источник
Характеристики объекта: • наименование и назначение • тип и архитектура • адреса размещения • категории сетей электросвязи • операторы и (или) провайдеры • тип доступа к сети (проводной, беспроводный), протоколы взаимодействия • наименования программно-аппаратных средств и их количество • наименование общесистемного программного обеспечения • наименования прикладных программ • функциональная схема • сетевая схема	ИТ-подразделение

Оформление результатов категорирования объектов КИИ и подготовка документов для ФСТЭК России

Информация	Источник
Характеристика мер защиты информации: • применяемые средства защиты информации • сведения о применяемых орг. мерах защиты информации • реквизиты сертификатов соответствия, иных документов	Служба ИБ

Подразделения, участвующие в категорировании объектов КИИ

- Администрация
- Аналитические подразделения
- Бухгалтерский и налоговый учет
- Внутренний контроль
- Делопроизводство
- Договорной отдел
- ИТ-подразделение
- Кадровая служба
- Методологическое подразделение
- Подразделение оп охране окружающей среды
- Подразделение по ГОиЧС
- Подразделение риск-менеджмента
- Подразделения статистики
- Представители структурных подразделений — основные виды деятельности
- Служба ИБ
- Финансово-экономическое подразделение
- Юридическая служба

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

t.me/pm_public

amonitoring.ru

Сергей Петров

Старший аналитик
обособленного подразделения
в г. Пенза компании
«Перспективный мониторинг»

Sergey.Petrov@amonitoring.ru