Что дальше

Приказ 235 ФСТЭК России

Приказ 239 ФСТЭК России

План деятельности

4.	**Управление инцидентами (Реагирование на компьютерные инциденты (ИНЦ))**
4.1.	Разработка Регламента Управления инцидентами (политики реагирования на компьютерные инциденты)
4.2.	Утверждение Регламента Управления инцидентами
4.3.	Определение персонального состава участников процесса Управления инцидентами , а также их назначение нормативным актом по организации
4.4	Непрерывный мониторинг, выявление и анализ компьютерных инцидентов
4.5	Уведомление ФСБ России об компьютерных инцидентах ИБ, выявленных в отношении объектов КИИ не являющихся значимыми, по электронной почте
4.6	Уведомление НКЦКИ об компьютерных инцидентах ИБ, выявленных в отношении значимых объектов КИИ с использованием ГосСОПКА
4.7	Разработка Регламента взаимодействия при реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак
4.8	Согласование Регламента взаимодействия при реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных с 8 Центром ФСБ России
4.9	Утверждение Регламента взаимодействия при реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак
4.10	Разработка Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
4.11	Утверждение Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
4.12	Корректировка Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
4.13	Информирование НКЦКИ о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак
4.14	Хранение и защита информации о компьютерных инцидентах

План деятельности

5.	**Создание и совершенствование системы безопасности значимых объектов КИИ**
5.1	Анализ угроз безопасности информации и разработка моделей угроз безопасности информации значимых объектов КИИ
5.2	Проектирование подсистем безопасности значимых объектов КИИ
5.3	Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности)
5.4	Внедрение подсистем безопасности значимых объектов КИИ
5.5	Подключение подсистем безопасности значимых объектов КИИ к ГосСОПКА
5.6	Модернизация (совершенствование) подсистем безопасности значимых объектов КИИ

6.	**Информирование и обучение персонала значимых объектов КИИ**
6.1	Разработка Политики информирования и обучения персонала (Регламента повышений уровня знаний)
6.2	Утверждение Политики информирования и обучения персонала
6.3	Определение персонального состава участников процесса информирования и обучения персонала значимых объектов КИИ
6.4	Формирование Плана проведения мероприятий по информированию и обучению персонала значимых объектов КИИ
6.5	Утверждение Плана проведения мероприятий по информированию и обучению персонала значимых объектов КИИ
6.6	Подготовка материалов, практических занятий для проведения мероприятий по информированию и обучению персонала значимых объектов КИИ
6.7	Проведение мероприятий по информированию и обучению персонала значимых объектов КИИ
6.8	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы

Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования

Приказ 235 ФСТЭК России

Приказ 235 ФСТЭК
Требования к созданию системы безопасности

- Общие положения
- Требования к силам обеспечения безопасности значимых объектов КИИ
- Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ
- Требования к организационно-распорядительным документам по безопасности значимых объектов
- Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ

Требования к созданию систем безопасности значимых объектов КИИ

Приказ 235 ФСТЭК России

2. Системы безопасности создаются субъектами критической информационной инфраструктуры и включают в себя правовые, организационные, технические и иные меры, направленные на обеспечение информационной безопасности (защиты информации) субъектов критической информационной инфраструктуры.

3. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак.

Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры для одного или группы значимых объектов критической информационной инфраструктуры могут создаваться отдельные системы безопасности.

4. Системы безопасности включают силы обеспечения безопасности значимых объектов критической информационной инфраструктуры и используемые ими средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Силы обеспечения безопасности значимых объектов

- подразделения (работники) субъекта КИИ, ответственные за обеспечение безопасности значимых объектов КИИ;
- подразделения (работники), эксплуатирующие значимые объекты КИИ;
- подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) значимых объектов КИИ;
- иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов КИИ.

Требования к силам обеспечения безопасности

Руководитель субъекта КИИ создает или определяет

- структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ (структурное подразделение по безопасности), или назначает
- отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ (специалисты по безопасности).

Обязанности структурного подразделения/специалиста по безопасности

- разрабатывать предложения по совершенствованию ОРД по безопасности значимых объектов и представлять их руководителю субъекта КИИ (уполномоченному лицу);
- проводить анализ угроз безопасности информации в отношении значимых объектов КИИ и выявлять уязвимости в них;
- обеспечивать реализацию требований по обеспечению безопасности значимых объектов КИИ;
- обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;
- осуществлять реагирование на компьютерные инциденты;
- организовывать проведение оценки соответствия значимых объектов КИИ требованиям по безопасности;
- готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов КИИ.

Требования к силам обеспечения безопасности

12. Работники структурного подразделения по безопасности, специалисты по безопасности должны обладать знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов критической информационной инфраструктуры в соответствии с настоящими Требованиями и требованиями по безопасности.

Требования к силам обеспечения безопасности

- Не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации.

Требования по обеспечению безопасности значимых объектов КИИ

Приказ 239 ФСТЭК России

9. На стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта проводятся:

а) задание требований к обеспечению безопасности значимого объекта;

б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;

в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;

г) обеспечение безопасности значимого объекта в ходе его эксплуатации;

д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Требования к программным и программно-аппаратным средствам

- Для обеспечения безопасности значимых объектов КИИ должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании"

Требования к программным и программно-аппаратным средствам

- Сертифицированные средства защиты информации применяются в случаях, установленных законодательством РФ, а также в случае принятия решения субъектом КИИ
- В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами КИИ самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством РФ лицензии на деятельность в области защиты информации.

Требования к программным и программно-аппаратным средствам

- Применяемые средства защиты информации должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

Требования к организационно-распорядительным документам по безопасности значимых объектов

Должны быть утверждены ОРД по безопасности значимых объектов, определяющие

- порядок и правила функционирования системы безопасности значимых объектов, а также
- порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры

ОРД по безопасности значимых объектов являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта КИИ

ОРД по безопасности значимых объектов должны определять

- а) цели и задачи обеспечения безопасности значимых объектов КИИ,
- основные угрозы безопасности информации и категории нарушителей,
- основные организационные и технические мероприятия по обеспечению безопасности значимых объектов КИИ, проводимые субъектом КИИ,
- состав и структуру системы безопасности и функции ее участников,
- порядок применения,
- формы оценки соответствия значимых объектов КИИ и средств защиты информации требованиям по безопасности;

ОРД по безопасности значимых объектов должны определять

- б) планы мероприятий по обеспечению безопасности значимых объектов КИИ,
- модели угроз безопасности информации в отношении значимых объектов КИИ,
- порядок реализации отдельных мер по обеспечению безопасности значимых объектов КИИ,
- порядок проведения испытаний или приемки средств защиты информации,
- порядок реагирования на компьютерные инциденты,
- порядок информирования и обучения работников,
- порядок взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов КИИ,
- порядок взаимодействия субъекта КИИ с ГосСОПКА;

ОРД по безопасности значимых объектов должны определять

- в) правила безопасной работы работников субъекта КИИ на значимых объектах КИИ,
- действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.

Состав и формы ОРД по безопасности значимых объектов определяются субъектом КИИ с учетом особенностей его деятельности.

Приказ 239 ФСТЭК России
Требования по обеспечению безопасности

12.2. Разрабатываемые ОРД по безопасности значимого объекта должны определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности), разработанных и внедренных в рамках подсистемы безопасности значимого объекта в соответствии с главой III настоящих Требований:

- 17 Политик

Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ

- планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ;
- реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов КИИ;
- контроль состояния безопасности значимых объектов КИИ;
- совершенствование безопасности значимых объектов КИИ.

Требования по обеспечению безопасности значимых объектов КИИ

Приказ 239 ФСТЭК России

Приказ 239 ФСТЭК
Требования по обеспечению безопасности

I. Общие положения

II. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

- Установление требований к обеспечению безопасности значимого объекта
- Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- Обеспечение безопасности значимого объекта в ходе его эксплуатации
- Обеспечение безопасности значимого объекта при выводе его из эксплуатации

III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение: Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Приказ 239 ФСТЭК

Стадии (этапы) жизненного цикла значимого объекта КИИ

- а) установление требований к обеспечению безопасности значимого объекта;
- б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;
- в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;
- г) обеспечение безопасности значимого объекта в ходе его эксплуатации;
- д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Результаты реализации мероприятий, проводимых для обеспечения безопасности значимого объекта на стадиях (этапах) его жизненного цикла, подлежат документированию.

Установление требований к обеспечению безопасности ЗО

- Задание требований к обеспечению безопасности значимого объекта осуществляется субъектом КИИ
- **Требования** к обеспечению безопасности **включаются в техническое задание** на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта.

Техническое задание

- а) цель и задачи обеспечения безопасности ЗО или подсистемы безопасности ЗО;
- б) категорию значимости ЗО;
- в) перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать ЗО;
- г) перечень типов объектов защиты ЗО;
- д) организационные и технические меры, применяемые для обеспечения безопасности ЗО;
- е) стадии (этапы работ) создания подсистемы безопасности ЗО;
- ж) требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
- з) требования к защите средств и систем, обеспечивающих функционирование ЗО (обеспечивающей инфраструктуре);
- и) требования к информационному взаимодействию ЗО с иными объектами КИИ, а также иными ИС, АСУ или ИТКС.

Разработка организационных и технических мер по обеспечению безопасности ЗО

- а) **анализ угроз безопасности информации** и **разработку модели угроз безопасности** информации или ее уточнение (при ее наличии);
- б) **проектирование подсистемы безопасности** значимого объекта;
- в) **разработку** рабочей (эксплуатационной) **документации** на значимый объект (в части обеспечения его безопасности).

Проектирование подсистемы безопасности ЗО

- а) **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) **и объекты доступа**;
- б) **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- в) **обосновываются организационные** и **технические меры**, подлежащие реализации в рамках подсистемы безопасности ЗО;
- г) **определяются виды и типы средств защиты информации**, обеспечивающие реализацию технических мер по обеспечению безопасности ЗО;
- д) **осуществляется выбор средств защиты информации** и (или) их разработка с учетом категории значимости ЗО, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;

Проектирование подсистемы безопасности ЗО

- е) **разрабатывается архитектура подсистемы безопасности** ЗО, включающая состав, места установки, взаимосвязи средств защиты информации;
- ж) **определяются требования к параметрам настройки** программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей ЗО;
- з) **определяются меры** по обеспечению **безопасности при взаимодействии** ЗО **с иными объектами** КИИ, ИС, АСУ или ИТКС.

Проектирование подсистемы безопасности ЗО

- В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды.

Разработка рабочей (эксплуатационной) документации на ЗО

- осуществляется в соответствии с техническим заданием
- должна содержать:
  - описание архитектуры подсистемы безопасности ЗО;
  - порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;
  - правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие

- а) **установку и настройку** средств защиты информации, настройку программных и программно-аппаратных средств;
- б) **разработку** организационно-распорядительных **документов**, регламентирующих правила и процедуры обеспечения безопасности ЗО;
- в) **внедрение организационных мер** по обеспечению безопасности ЗО;
- г) **предварительные испытания** ЗО и его подсистемы безопасности;
- д) **опытную эксплуатацию** ЗО и его подсистемы безопасности;
- е) **анализ уязвимостей** ЗО и принятие мер по их устранению;
- ж) **приемочные испытания** ЗО и его подсистемы безопасности.

Обеспечение безопасности ЗО в ходе его эксплуатации

- а) планирование мероприятий по обеспечению безопасности ЗО;
- б) анализ угроз безопасности информации в ЗО и последствий от их реализации;
- в) управление (администрирование) подсистемой безопасности ЗО;
- г) управление конфигурацией ЗО и его подсистемой безопасности;
- д) реагирование на компьютерные инциденты в ходе эксплуатации ЗО;
- е) обеспечение действий в нештатных ситуациях в ходе эксплуатации ЗО;
- ж) информирование и обучение персонала ЗО;
- з) контроль за обеспечением безопасности ЗО.

Информирование и обучение персонала значимого объекта

- а) информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации ЗО;
- б) доведение до персонала требований по обеспечению безопасности ЗО, а также положений организационно-распорядительных документов по безопасности ЗО;
- в) обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;
- г) контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности КИИ.

Средства защиты

28. Для обеспечения безопасности значимых объектов КИИ должны применяться средства защиты информации, **прошедшие оценку** на соответствие требованиям по безопасности **в формах обязательной сертификации**, **испытаний** или **приемки**.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом КИИ.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами КИИ самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

Испытания (приемка) средств защиты информации проводятся отдельно или в составе значимого объекта КИИ в соответствии с программой и методиками испытаний (приемки), утверждаемыми субъектом КИИ.

Обеспечение безопасности ЗО при выводе его из эксплуатации

- а) архивирование информации, содержащейся в ЗО;
- б) уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;
- в) уничтожение данных об архитектуре и конфигурации ЗО;
- г) архивирование или уничтожение эксплуатационной документации на ЗО и его подсистему безопасности и организационно-распорядительных документов по безопасности ЗО.

Архивирование информации, содержащейся в ЗО, должно осуществляться в случае ее дальнейшего использования в деятельности субъекта КИИ.

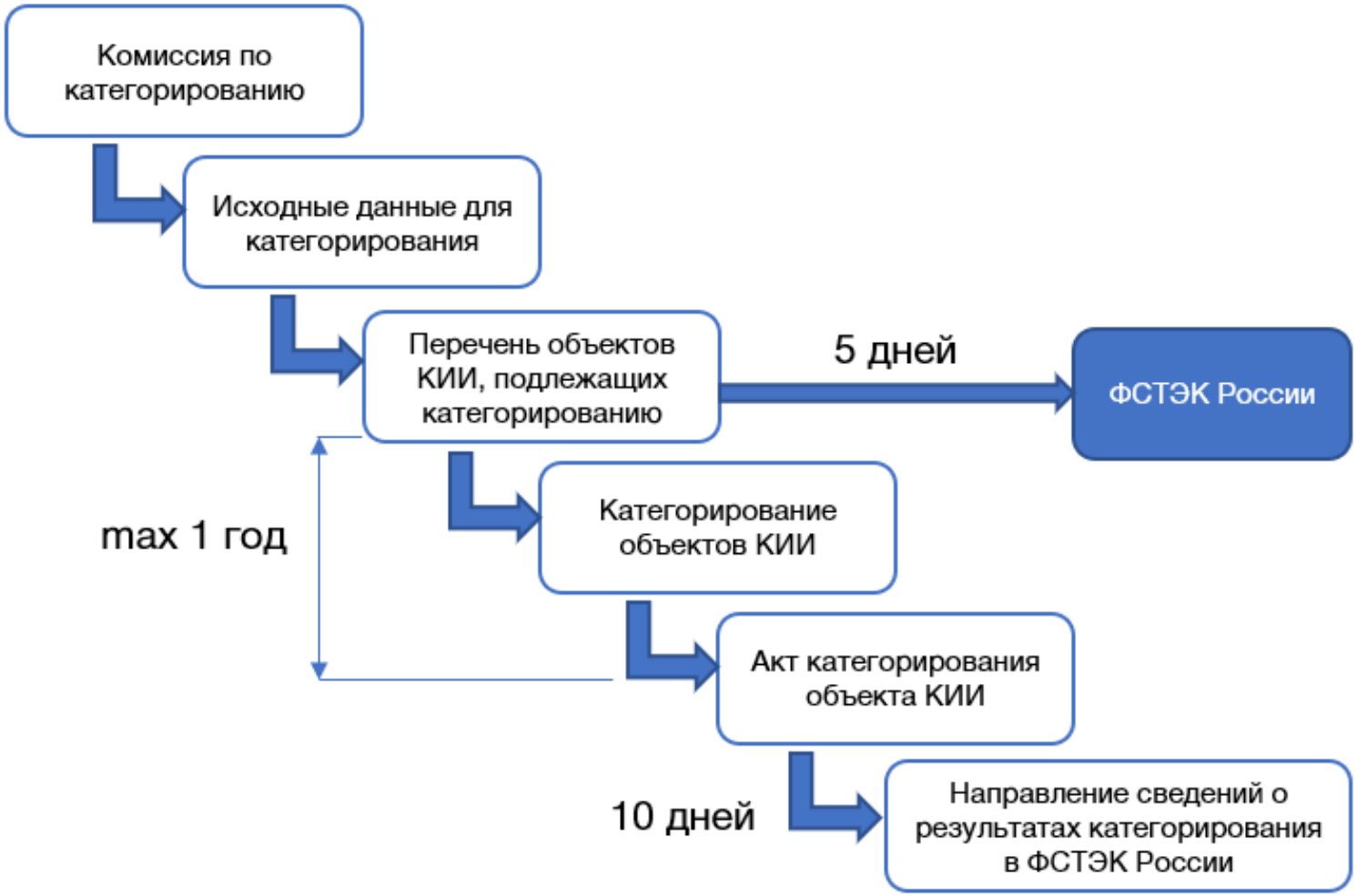
Организационные и технические меры

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты информационной безопасности (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
II. Управление доступом (УПД)				
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступом	+	+	+
УПД.3	Доверенная загрузка		+	+

Порядок категорирования объектов КИИ



Вопросы?

Спасибо за внимание!

Игорь Михайлович Бирюк

Институт МОИБ

8 (495) 268-13-42

info@imoib.ru

imoib.ru

Институт мониторинга и оценки информационной безопасности