Эшелон
комплексная безопасность

# Требования к защите информации, содержащейся в государственных ИС, в контексте изменений в Приказ ФСТЭК России от 11.02.2013 № 17

**Васильев Петр**
Директор департамента аттестации
АО «НПО «Эшелон»

# ЧТО НОВОГО ?

**Приказ ФСТЭК России от 15 февраля 2017 г. № 27**

«О внесении **изменений** в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17»

- **3 класса** защищенности ГИС;
- Применение **БДУ ФСТЭК** России при **определении угроз БИ**;
- **Изменения** в части содержания **ТЗ** на создание СЗИ;
- Меры по **нейтрализации известных уязвимостей** при внедрении СЗИ;
- Размещение ГИС только в **аттестованном ЦОД**;
- Некоторые **организационные вопросы**, связанные с **проектированием** и **аттестацией**;
- **Применение СрЗИ** с соответствующими классу ГИС **функциями безопасности**.

Эшелон
комплексная безопасность

# 1. КЛАССИФИКАЦИЯ ГИС

**п. 14.2 – 3 класса защищенности ГИС**

+ изменения в Приложение № 1 к Приказу (классификация)

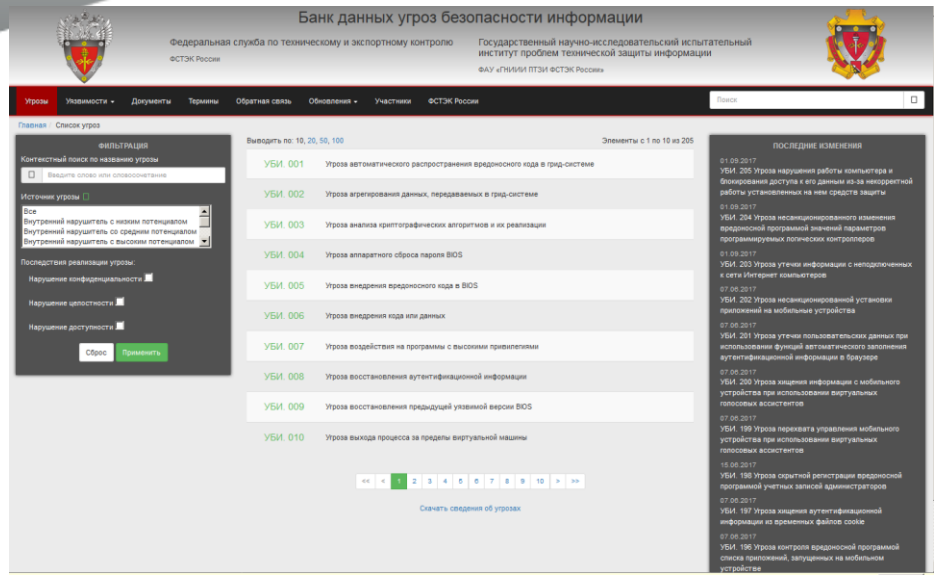
+ изменения в Базовый состав мер защиты информации (Приложение № 2 к Приказу)

| УПД.3 Управление информационными потоками … | | |
|---|---|---|
| **3** | 2 | 1 |
| **+** | + | + |

| ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты … | | |
|---|---|---|
| **3** | 2 | 1 |
| **+** | + | + |

Эшелон
комплексная безопасность

# 2. ОПРЕДЕЛЕНИЕ УГРОЗ БИ




п. 14.3:

…

В качестве исходных данных для определения угроз безопасности информации используются:

- банк данных угроз безопасности информации (bdu.fstec.ru);
- а так же иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

! «Методика определения угроз БИ в ИС» ФСТЭК Р – статус проекта 2015 года ?

OWASP
Open Web Application Security Project

Эшелон
комплексная безопасность

# 3. СОДЕРЖАНИЕ ТЗ

п. 14.4:

…

- стадии (этапы работ) создания системы защиты информационной системы;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
- функции заказчика и оператора по обеспечению защиты информации в информационной системе;
- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);

…

# 3.1 СОГЛАСОВАНИЕ ДОКУМЕНТОВ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

**О порядке рассмотрения и согласования моделей угроз безопасности информации и технических заданий на создание государственных информационных систем**

от 22 июня 2017 г. N 240/22/3031

**Постановление Правительства Российской Федерации от 11 мая 2017 г. N 555**

Рассмотрение и согласование МУ и ТЗ на создание федеральных ИС - **осуществляется центральным аппаратом ФСТЭК России.**
Рассмотрение и согласование МУ и ТЗ на создание региональных ИС - **осуществляется управлениями ФСТЭК России по федеральным округам.**

Эшелон
комплексная безопасность

# 4. АНАЛИЗ УЯЗВИМОСТЕЙ

**Внедрение СЗИ**

п. 16.6

…

По результатам анализа уязвимостей **должно быть подтверждено**, что в информационной системе **отсутствуют уязвимости**, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их **использование** (эксплуатация) нарушителем **невозможно.**

**Аттестация ГИС**

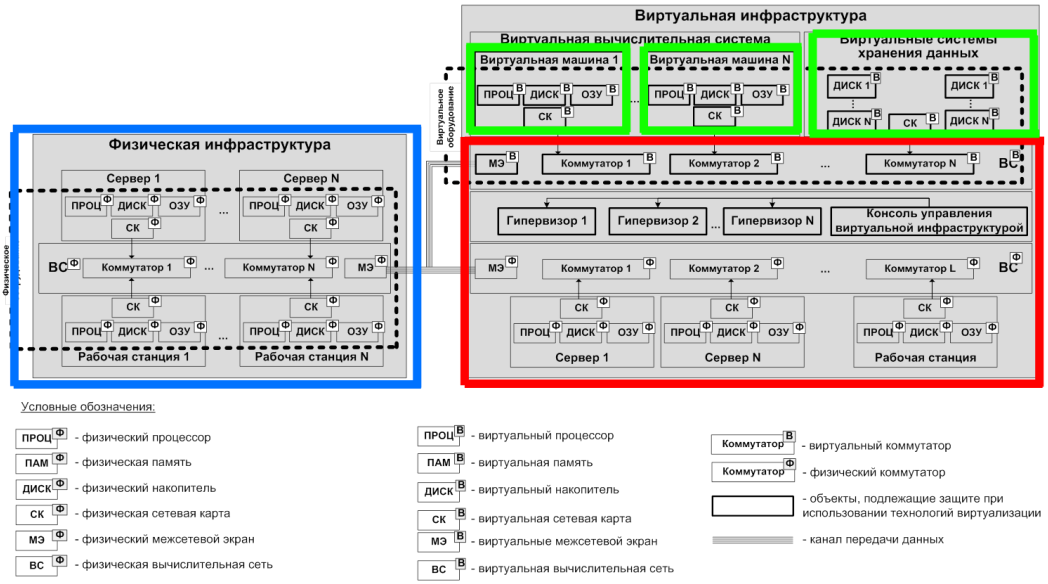
п. 17.2

При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

…

- **анализ уязвимостей информационной системы**, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации.

# 5. АТТЕСТАЦИЯ (1)




17.6. Информационные системы, функционирующие **на базе общей инфраструктуры** (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, **подлежат аттестации** в составе указанной инфраструктуры.

В случае, если информационная система создается на базе **центра обработки данных** уполномоченного лица, такой **центр обработки данных должен быть аттестован** по классу защищенности не ниже класса защищенности, установленного для создаваемой информационной системы.

Эшелон
комплексная безопасность

# 5.1 АТТЕСТАЦИЯ (2)

17. Проведение аттестационных испытаний информационной системы **должностными лицами**, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, **не допускается**.

17.4. Повторная аттестация информационной системы осуществляется по окончании срока действия аттестата соответствия, **который не может превышать 5 лет**, или повышения класса защищенности информационной системы.

# 6. ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

| Класс ГИС / Класс СрЗИ | 3 | 2 | 1 |
|---|---|---|---|
| Класс СрЗИ (ПЗ ФСТЭК) | Не ниже 6 | Не ниже 5 | Не ниже 4 |
| Класс СВТ (РД СВТ 1992) | Не ниже 5 | | |
| Уровень контроля НДВ (1999) | --- | Не ниже 4 | |

п. 26:
В информационных системах применяются средства защиты информации, **сертифицированные на соответствие обязательным требованиям** по безопасности информации, **установленным ФСТЭК России**, или на **соответствие требованиям**, указанным в **технических условиях (заданиях по безопасности)**. При этом **функции безопасности** таких средств **должны обеспечивать выполнение** настоящих Требований.

Эшелон
комплексная безопасность

НАУЧНЫЙ, ПРАКТИЧЕСКИЙ, ПЕРИОДИЧЕСКИЙ, РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

# Благодарю за внимание!

Москва, ул. Электрозаводская, д. 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.npo-echelon.ru

mail@npo-echelon.ru