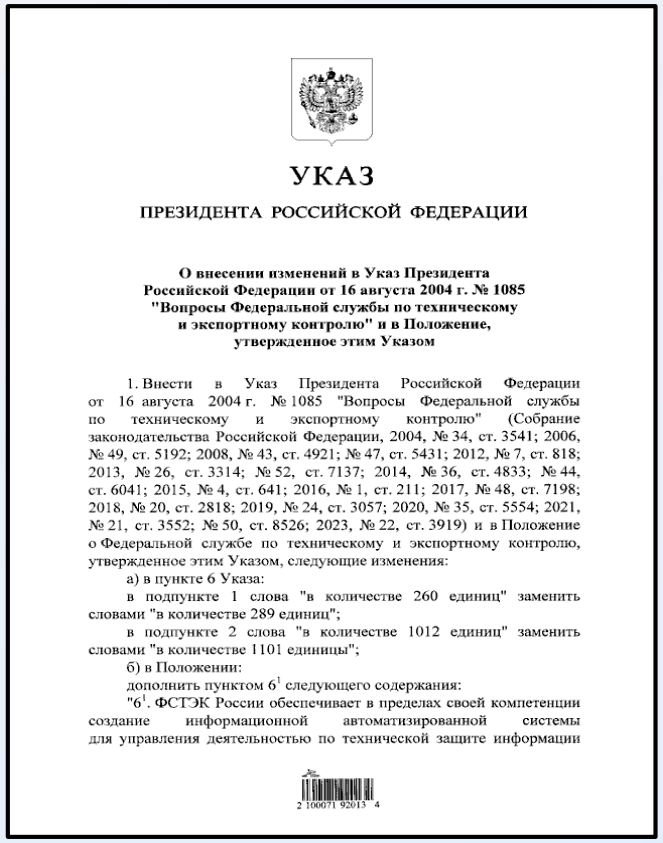
О МЕТОДИЧЕСКОМ ПОДХОДЕ К ОЦЕНКЕ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНИЗАЦИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Жиров Павел Валентинович

Заместитель начальника управления ФСТЭК России

ОЦЕНКА ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНИЗАЦИЙ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" и в Положение, утвержденное этим Указом

1. Внести в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818; 2019, № 24, ст. 3057; 2020, № 35, ст. 5554; 2021, № 21, ст. 3552; № 50, ст. 8526; 2023, № 22, ст. 3919) и в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное этим Указом, следующие изменения:

а) в пункте 6 Указа:

в подпункте 1 слова "в количестве 260 единиц" заменить словами "в количестве 289 единиц";

в подпункте 2 слова "в количестве 1012 единиц" заменить словами "в количестве 1101 единицы";

б) в Положении:

дополнить пунктом 6^1 следующего содержания:

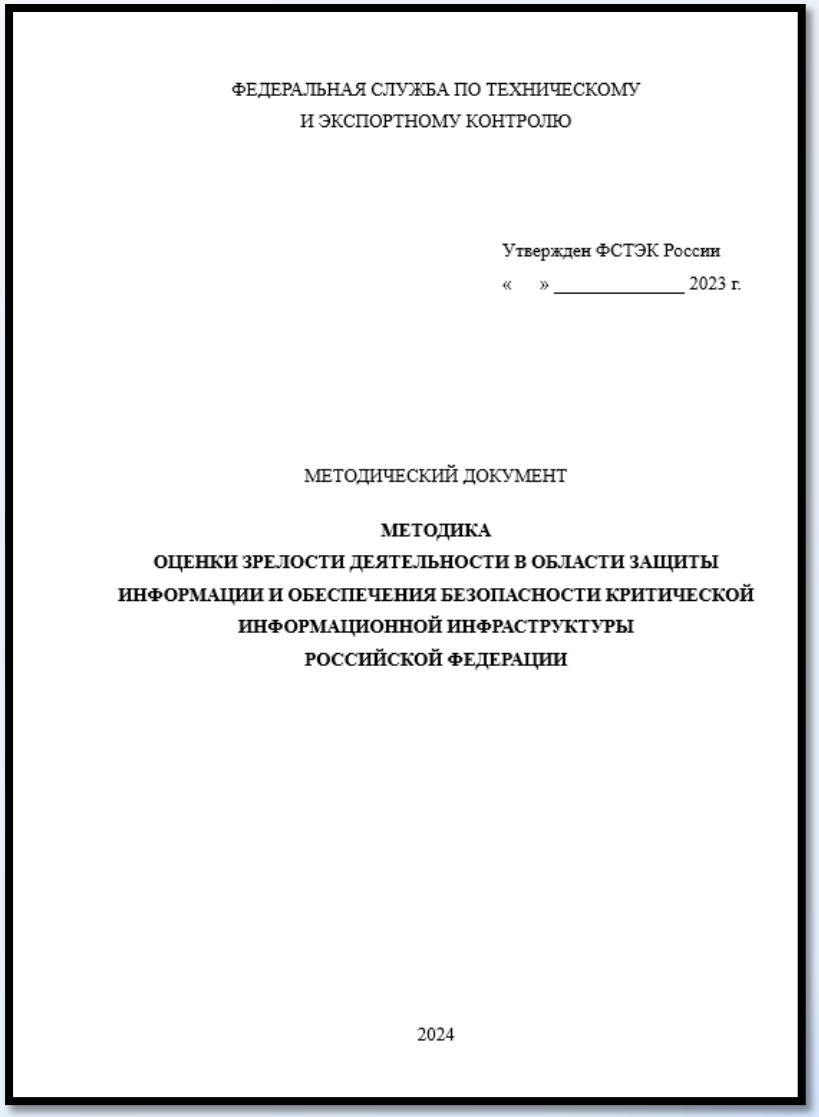
"6^1. ФСТЭК России обеспечивает в пределах своей компетенции создание информационной автоматизированной системы для управления деятельностью по технической защите информации

2 100071 92013 4

Организация и проведение оценки эффективности деятельности органов государственной власти и организаций по технической защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры

Показатель зрелости деятельности в области защиты информации и обеспечения безопасности критической информационной инфраструктуры Российской Федерации

МЕТОДИКА ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
« » _____ 2023 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

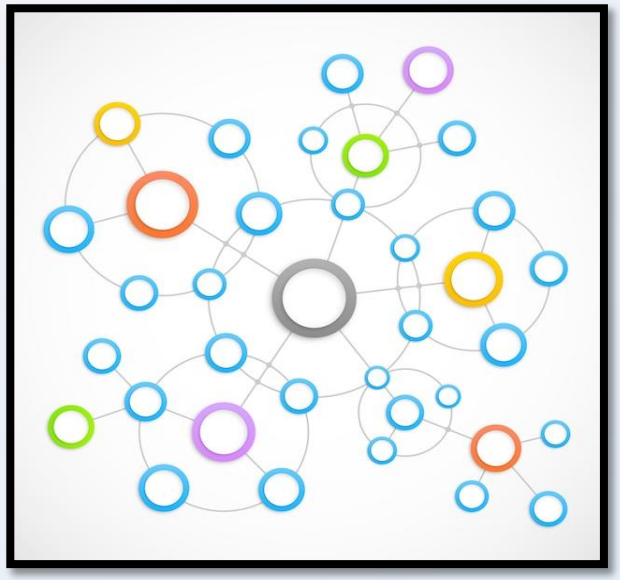
**МЕТОДИКА
ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**

2024

Применяется для оценки деятельности заместителя руководителя органа (организации), на которого возложены полномочия по обеспечению информационной безопасности органа (организации), и (или) структурного подразделения, осуществляющего функции по обеспечению информационной безопасности органа (организации)

Определяет показатели зрелости деятельности государственного органа, органа местного самоуправления, организации, в том числе субъекта критической информационной инфраструктуры по защите информации, не составляющей государственную тайну, и (или) обеспечению безопасности значимых объектов критической информационной инфраструктуры, а также порядок расчета показателя зрелости.

СХЕМА ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ



Модель оценки

- Поле оценки → Основные направления информационной безопасности
- Уровни оценки зрелости → Несистемный; Повторяемый; Управляемый; Верифицируемый
- Критерии оценки → Фактическая реализация; Документирование; Контроль реализации; Актуализация реализации

ПОЛЕ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

№	Наименование основных направлений ИБ
1	Планирование мероприятий по защите информации
2	Моделирование угроз безопасности информации (в том числе кибер-разведка TI)
3	Повышение уровня осведомленности работников в сфере информационной безопасности и обучение
4	Физическая защита объектов
5	Обеспечение непрерывности деятельности (в том числе резервирование)
6	Резервное копирование
7	Безопасность обмена информацией
8	Шифрование данных
9	Защита электронной почты
10	Безопасное удаление данных
11	Безопасность оборудования (HW security)
12	Безопасность конечных устройств (безопасная настройка, контроль целостности, доверенная загрузка, ограничения программной среды)
13	Защита мобильных устройств (MDM)
14	Защита контейнерных сред
15	Безопасность средств виртуализации
16	Антивирусная защита
17	Защита каналов связи (в том числе VPN) и межсетевого взаимодействия
18	Межсетевое экранирование (FW,NGFW,IPS/IDS, sandbox)
19	Идентификация/аутентификация и управление доступом (2FA, PAM, IAM)
20	Управление паролями и секретами
21	Мониторинг событий и управление инцидентами информационной безопасности
22	Безопасная разработка (SSDLC, appsec, багбаунти)

УРОВНИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

№	Уровень зрелости	Принципиальное определение	Пояснение по критериям зрелости
1	**Несистемный**	Требования к мерам ИБ реализуются частично или с нарушениями. Система процессов управления ИБ не выстроена. Документирование носит отрывочный характер.	Реализация: частичная/с нарушениями, местами полная Документы: частично/не соответствуют действительности и/или НПА Контроль: административный, преимущественно исполнительской дисциплины Актуализация: большая часть ОРД не пересматривается, требования и меры не актуализируются
2	**Повторяемый**	Реализация мер ИБ документирована в ОРД, контролируется и пересматривается в соответствии с изменениями и/или целями органа (организации)	Реализация: соответствует НПА, процессы выстроены/внедряются Документы: соответствуют мерам/процессам и требованиям НПА Контроль: в основном административный, иногда измеримый Актуализация: регулярная, иногда частичная, в основном пересмотр ОРД согласно изменений/целей органа (организации)
3	**Управляемый**	Управление мерами ИБ построено на регулярном пересмотре рисков/моделировании актуальных угроз	Реализация: требования выполняются, меры корректируются согласно ландшафта угроз/рисков, процессы увязаны в систему Документы: определяют процессы и актуальные требования к мерам ИБ Контроль: измеримый, результативности мер и соответствия требованиям Актуализация: регулярная; пересмотр мер/процессов/требований и ОРД согласно актуальных угроз
4	**Верифицируемый**	Управление мерами ИБ построено на анализе ущерба/негативных последствий с верификацией реализуемости потенциальных угроз ИБ	Реализация: требования выполняются, меры управляются согласно актуальных угроз, процессы увязаны в систему. Документы: определяют процессы и актуальные требования к мерам ИБ Контроль: измеримый, результативности мер и соответствия требованиям с практической проверкой защиты от негативных последствий Актуализация: регулярная; пересмотр мер/процессов/угроз/требований и ОРД согласно актуальной карты негативных последствий

КРИТЕРИИ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Направление ИБ	Критерии оценки	Значение
Планирование мероприятий по защите информации	**Фактическая реализация (люди, процессы, технологии)**	Выполняется планирование развития ИБ (возможно неформально). В органе (организации) имеется видение по развитию системы обеспечения ИБ. Выделяется средства на нужды ИБ (как минимум фонд оплаты труда, закупка СЗИ и т.д.). Определены цели ИБ (возможно неформально).
	Документальное обеспечение реализации	Разработан план развития ИБ в органе (организации) (возможно неформальный, в виде рабочего документа или переписки)
	Контроль реализации	Высшим руководством проводится оценка достаточности выделенного бюджета на нужды ИБ.
	Актуализация реализации	Высшим руководством принимаются решения об изменении бюджетирования на нужды ИБ (как минимум по необходимости или по инициативе работников, по запросу).

ПОРЯДОК ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сбор и анализ исходных данных

Расчет показателей зрелости деятельности и его сравнение с базовым и целевым профилем уровня зрелости

Определение итоговой оценки зрелости органа (организации)

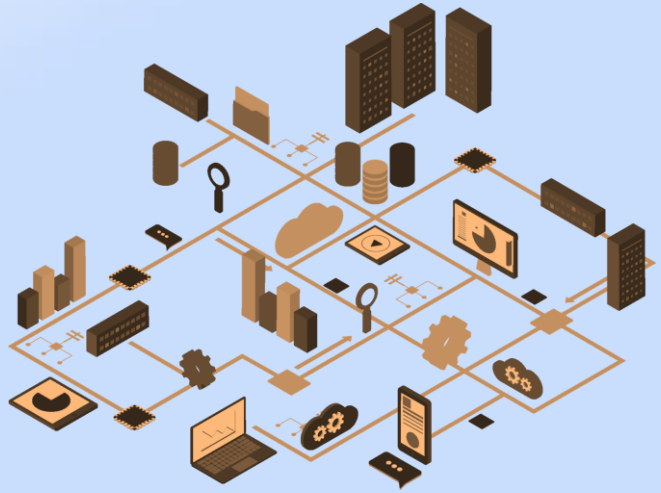
СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ

Отчеты, протоколы, иные документы, составленные по результатам внутреннего контроля уровня защиты информации (обеспечения безопасности)

Акты, протоколы, иные документы, составленные по результатам государственного контроля в области обеспечения безопасности

Отчеты, составленные по результатам внешней оценки соответствии в области обеспечения безопасности (аудита безопасности)

Внутренние организационно-распорядительные документы, регламентирующие обеспечение безопасности в органе (организации)



Результаты проведения инвентаризации информационной инфраструктуры

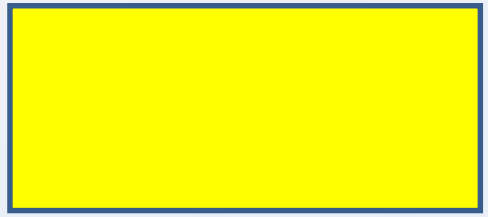
РАСЧЕТ ПОКАЗАТЕЛЕЙ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ И ЕГО СРАВНЕНИЕ С БАЗОВЫМ И ЦЕЛЕВЫМ ПРОФИЛЕМ

Целевой профиль

Базовый профиль

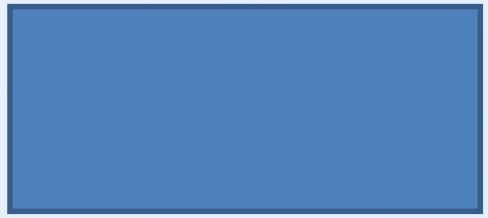
ОПРЕДЕЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНА (ОРГАНИЗАЦИИ)

Не достигнут базовый уровень
(выявлен хоть один недостаток реализации базового профиля по любой из мер защиты).



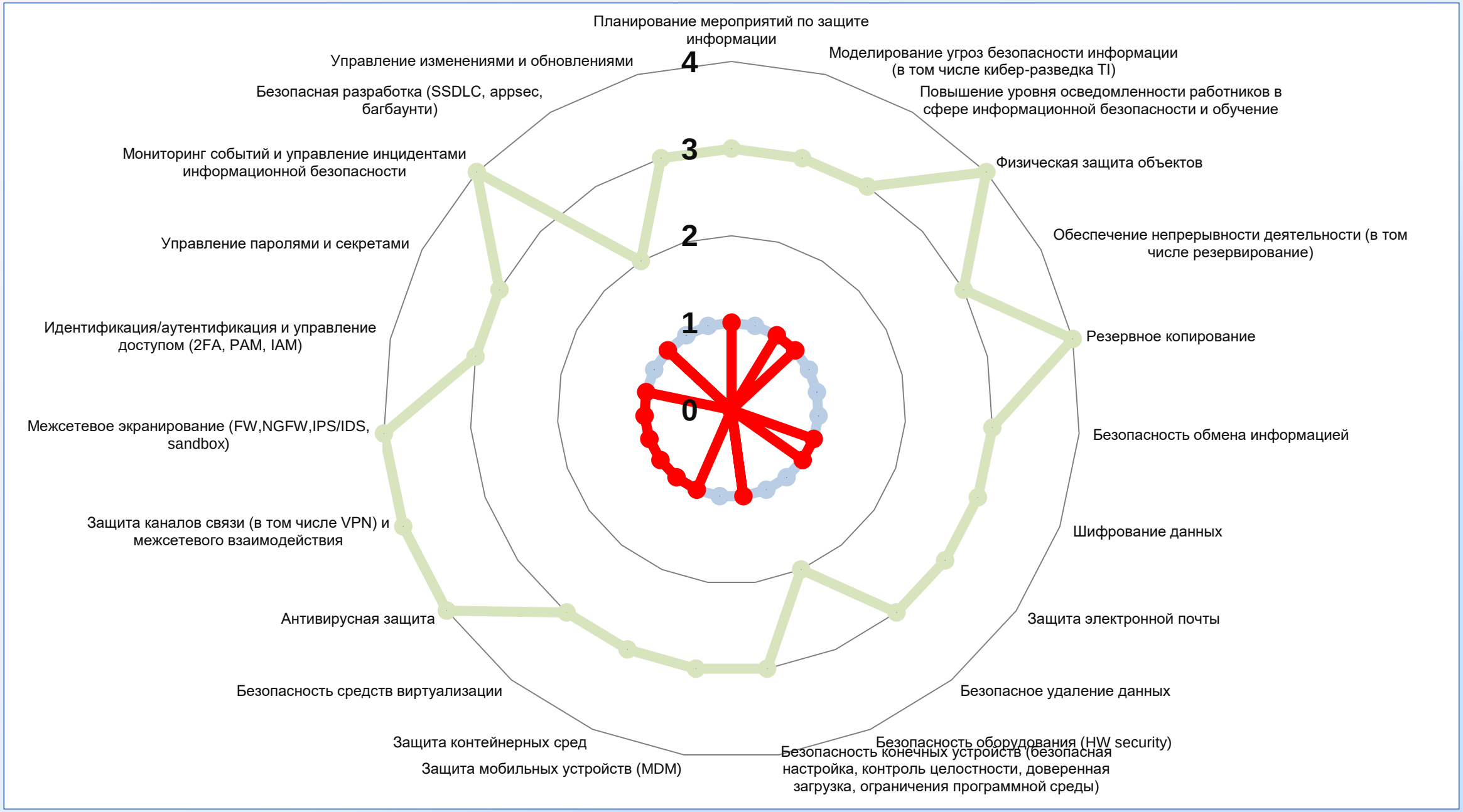
Базовый уровень полностью достигнут (нет недостатков), все оценки находятся между базовым уровнем и целевым профилем; меньше 65 % мер достигли целевого эффективности

Базовый уровень реализован, целевой профиль достигнут полностью или с несущественными отклонениями (все оценки находятся близко к целевому профилю или выше). Больше 65% мер с достижением целевого уровня.

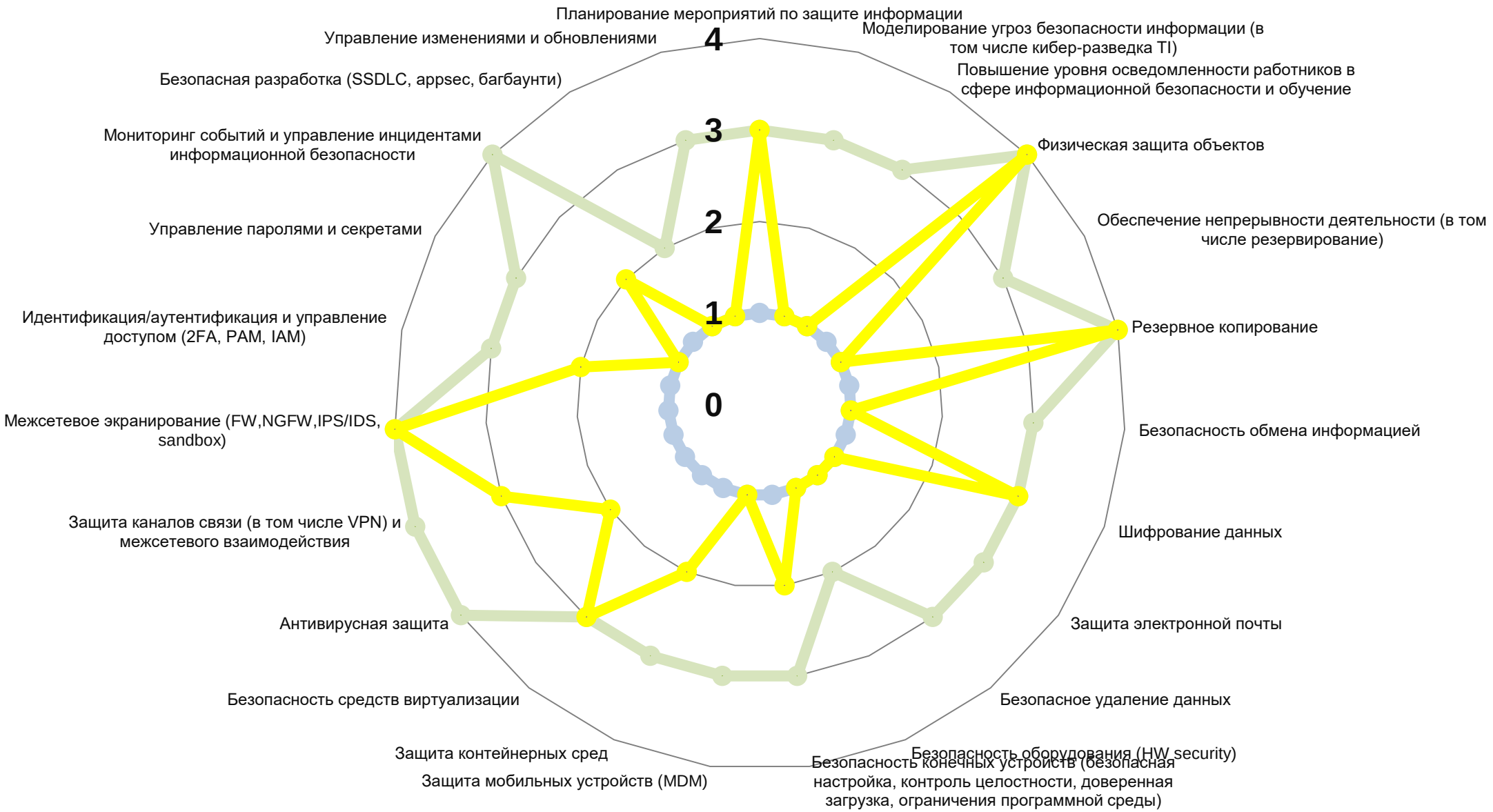


Достигнут полностью уровень целевого профиля зрелости или превосходит его

ОПРЕДЕЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНА (ОРГАНИЗАЦИИ)

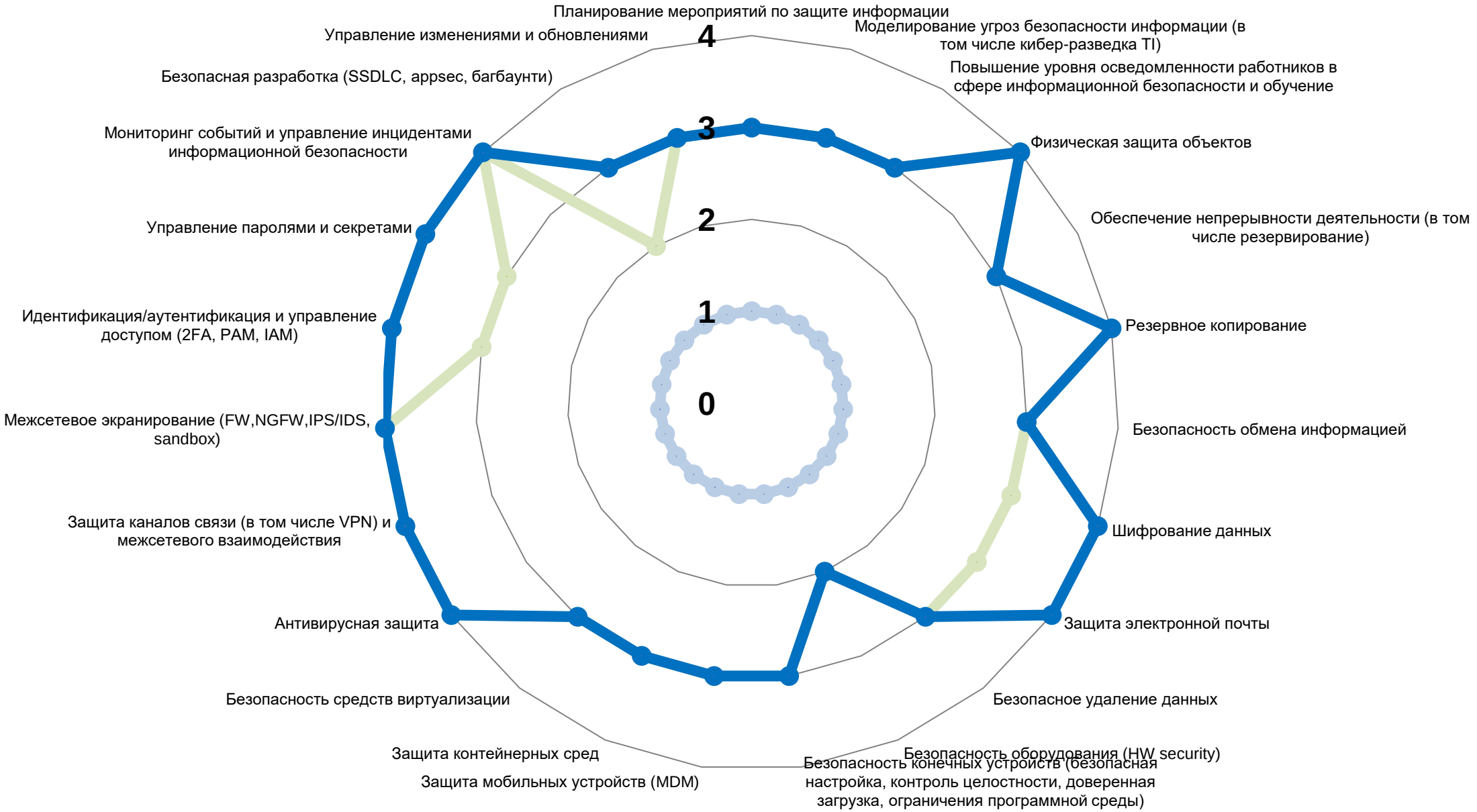


ОПРЕДЕЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНА (ОРГАНИЗАЦИИ)



ОПРЕДЕЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНА (ОРГАНИЗАЦИИ)

ОПРЕДЕЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНА (ОРГАНИЗАЦИИ)



О МЕТОДИЧЕСКОМ ПОДХОДЕ К ОЦЕНКЕ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНИЗАЦИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Жиров Павел Валентинович

Заместитель начальника управления ФСТЭК России