



РусКрипто

XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ

МЕТОДИКА ОЦЕНКИ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Домуховский Николай Анатольевич
Старший преподаватель УрФУ



Существующие методики оценки





Существующие методики оценки: сравнение

Методика	Охват всех требований в области КИИ	Охват различных направлений контроля	Возможность расчета количественной оценки	Использование объективных критериев	Возможность приоритизации выявленных нарушений
СТО БР ИББС-1.2-2014	низкий	высокий	высокая	среднее	низкая
Методика НКЦКИ	низкий	низкий	низкая	низкое	низкая
ГОСТ Р 57580.2-2018	низкий	высокий	высокая	среднее	низкая
Методика ФСТЭК России	средний	низкий	высокая	высокое	низкая



Требования к разрабатываемой методике оценки

Методика	Охват всех требований в области КИИ	Охват различных направлений контроля	Возможность расчета количественной оценки	Использование объективных критериев	Возможность приоритизации выявленных нарушений
Разрабатываемая методика	ВЫСОКИЙ	ВЫСОКИЙ	ВЫСОКАЯ	ВЫСОКОЕ	ВЫСОКАЯ
	Проверка выполнения всех актуальных требований НПА в области обеспечения безопасности ЗО КИИ	Проверка как состояния технических объектов, так и организационных процессов	Вычисление итоговой оценки состояния безопасности ЗО КИИ по заданному алгоритму	Расчет оценок показателей с использованием количественных метрик с опорой на свидетельства выполнения требований	Использование варьируемых весовых коэффициентов



Источники требований по обеспечению безопасности ЗО КИИ

187-ФЗ

Постановления
Правительства РФ № 127,
162, 1272, 1478, 1912

Указы Президента РФ
№ 250, 166

Приказы ФСТЭК России
№ 235, 239

Приказы ФСБ России

Распоряжение Секретаря
Совета Безопасности РФ

Порядка 400 неструктурированных требований



Иерархия требований

Процесс	Категорирование объектов КИИ
Подпроцесс	Создание в организации постоянно действующей комиссии по категорированию объектов КИИ
Требования	Решением руководителя субъекта КИИ (приказ по организации) создана постоянно действующая комиссия по категорированию объектов КИИ
	Состав постоянно действующей комиссии по категорированию объектов КИИ актуален на момент оценки
	В состав комиссии входит руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо

...



Группировка требований по процессам

организационно-
распорядительное и
нормативное обеспечение
безопасности объектов КИИ

(1 подпроцесс,
20 требований)

P_Name_1

P_Name_2

P_Name_3

P_Name_4

P_Name_5

P_Name_6

P_Name_7

P_Name_8

P_Name_9

управление системой
обеспечения безопасности
объектов КИИ

(8 подпроцессов,
49 требований)

установление уровней
опасности, обнаружение
компьютерных инцидентов и
реагирование на них

(6 подпроцессов,
48 требований)

обеспечение безопасности
объектов КИИ
с использованием
технических средств

(23 подпроцесса,
98 требований)

категорирование
объектов КИИ

(7 подпроцессов,
43 требования)

создание сил
обеспечения
безопасности
объектов КИИ

(6 подпроцессов,
23 требования)

организация контроля
выполнения
требований

(5 подпроцессов,
29 требований)

выполнение требований
нормативных правовых
актов, предъявляемых к
объектам КИИ

(14 подпроцессов,
74 требования)

обеспечение
физической
безопасности
объектов КИИ

(4 подпроцесса,
12 требований)



Алгоритм расчета оценки состояния безопасности ЗО КИИ

- 1 Задать значения весовых коэффициентов требований НПА
- 2 Задать значения весовых коэффициентов подпроцессов обеспечения безопасности
- 3 Задать значения весовых коэффициентов процессов обеспечения безопасности
- 4 Выставить значения оценок выполнения требований НПА
- 5 Вычислить оценки подпроцессов обеспечения безопасности
- 6 Вычислить оценки процессов обеспечения безопасности
- 7 Вычислить итоговое значение оценки обеспечения безопасности ЗО КИИ



Количественная оценка

- 1 Весовые коэффициенты требований НПА:
 $(W_{k,i,j}^{(Ep)})$, при этом весовые коэффициенты лежат в диапазоне от 0 до 1 и не могут одновременно равняться 0
 - 2 Весовые коэффициенты подпроцессов:
 $(W_{k,i}^{(Ep)})$, при этом весовые коэффициенты лежат в диапазоне от 0 до 1 и не могут одновременно равняться 0
 - 3 Весовые коэффициенты процессов:
 (W_k) , при этом весовые коэффициенты лежат в диапазоне от 0 до 1 и не могут одновременно равняться 0
- K – количество процессов обеспечения безопасности ЗО КИИ
(в рассматриваемом случае $K = 9$)
- $k = \overline{1, K}, \quad i = \overline{1, I_k}, \quad j = \overline{1, J_{k,i}}$
- I_k – количество подпроцессов, выделенных в k -ом процессе
- $J_{k,i}$ – количество требований, отнесенных к i -му подпроцессу k -го процесса



Значения весовых коэффициентов

0,4

«Низкая
значимость»

0,7

«Средняя
значимость»

1,0

«Высокая
значимость»

значение «0» (требование не применяется) не используется



Количественная оценка (продолжение)

4 Оценки выполнения требований:

$$V_{k,i,j} = \begin{cases} 1, & \text{если } (k, i, j)\text{-ое требование выполняется,} \\ 0, & \text{если } (k, i, j)\text{-ое требование не выполняется} \end{cases}$$

5 Оценки подпроцессов обеспечения безопасности ЗО КИИ:

$$Epp_{k,i} = \frac{\sum_{j=1}^{J_{k,i}} V_{k,i,j} W_{k,i,j}^{(Epp)}}{\sum_{j=1}^{J_{k,i}} W_{k,i,j}^{(Epp)}}$$

6 Оценки процессов обеспечения безопасности ЗО КИИ:

$$Ep_k = \frac{\sum_{i=1}^{I_k} Epp_{k,i} W_{k,i}^{(Ep)}}{\sum_{i=1}^{I_k} W_{k,i}^{(Ep)}}$$

7 Итоговое значение оценки обеспечения безопасности ЗО КИИ:

$$E = \frac{\sum_{k=1}^K Ep_k W_k}{\sum_{k=1}^K W_k}$$



Итоговая оценка

Полностью
соответствует

$$0,9 \leq E \leq 1$$

В основном
соответствует

$$0,75 \leq E < 0,9$$

Не в полной мере
соответствует

$$0,5 \leq E < 0,75$$

Не
соответствует

$$0 \leq E < 0,75$$

Допускается изменение значений границ уровней исходя из специфики организации
и/или объекта КИИ

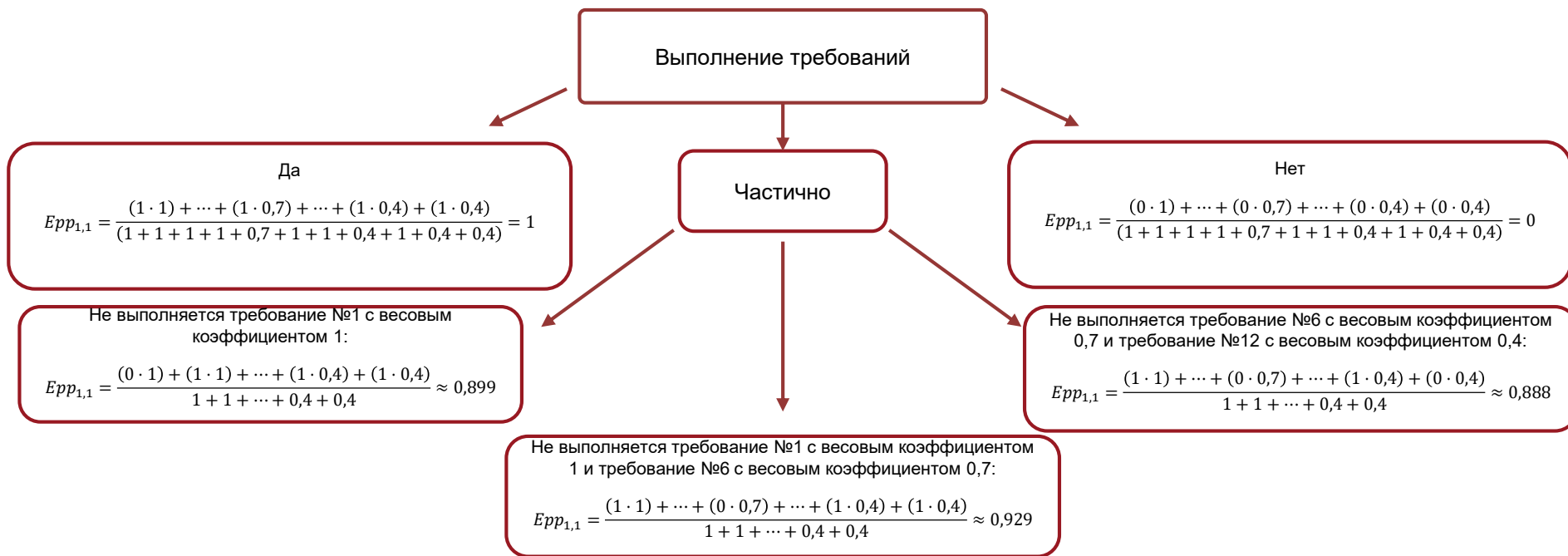


Пример расчета

№ п/п (j)	Требования безопасности подпроцесса «Создание в организации постоянно действующей комиссии по категорированию объектов КИИ»	$V_{1,1,j}$ при ответе «да»	$V_{1,1,j}$ при ответе «нет»	Весовой коэффициент
1	Решением руководителя субъекта КИИ (приказ по организации) создана постоянно действующая комиссия по категорированию объектов КИИ	1	0	1
2	Состав постоянно действующей комиссии по категорированию объектов КИИ актуален на момент оценки	1	0	1
3	В состав комиссии входит руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо	1	0	1
4	Комиссию по категорированию возглавляет руководитель субъекта КИИ или уполномоченное им лицо	1	0	1
5	В состав комиссии входят работники субъекта КИИ, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности	1	0	1
6	В состав комиссии входят работники субъекта КИИ, являющиеся специалистами в области в области связи	1	0	0,7
7	В состав комиссии входят работники субъекта КИИ, являющиеся специалистами в области в области информационных технологий	1	0	1
8	В состав комиссии входят работники субъекта КИИ, являющиеся специалистами по эксплуатации основного технологического оборудования	1	0	1
9	В состав комиссии входят работники субъекта КИИ, являющиеся специалистами в области технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов	1	0	0,4
10	В состав комиссии входят работники субъекта КИИ, на которых возложены функции обеспечения безопасности (ИБ) объектов КИИ	1	0	1
11	В состав комиссии входят работники подразделения по защите государственной тайны субъекта КИИ (в случае, если объект КИИ обрабатывает информацию, составляющую государственную тайну)	1	0	0,4
12	В состав комиссии входят работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций	1	0	0,4



Пример расчета (продолжение)



Таким образом, $Epp_{1,1} \in [0, 1]$, где 0 означает «не выполняется ни одно из требований подпроцесса», 1 означает «выполняются все требования подпроцесса»



Преимущества методики

01 Полнота контроля требований

- Учтено многообразие требований в области обеспечения безопасности ЗО КИИ (как технических, так и организационных)

02 Сопоставимость и воспроизводимость оценок

- Обеспечены сопоставимость и воспроизводимость оценок при проведении анализа выполнения требований НПА в различных субъектах КИИ и группах предприятий

03 Приоритизация нарушений

- Реализована возможность приоритизации нарушений по степени влияния на итоговую оценку для учета при выдаче обоснованных рекомендаций на основе веса требования

04 Практическая значимость

- Обеспечена возможность реализации методики в составе программно-технического средства контроля обеспечения безопасности ЗО КИИ

05 Распределение ответственности

- Разделение оценок по процессам и подпроцессам позволяет распределить задачу контроля обеспечения безопасности ЗО КИИ в соответствии с компетенциями опрашиваемых



РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Спасибо за внимание!

Домуховский Николай Анатольевич
Старший преподаватель УрФУ
n.a.domukhovsky@urfu.ru