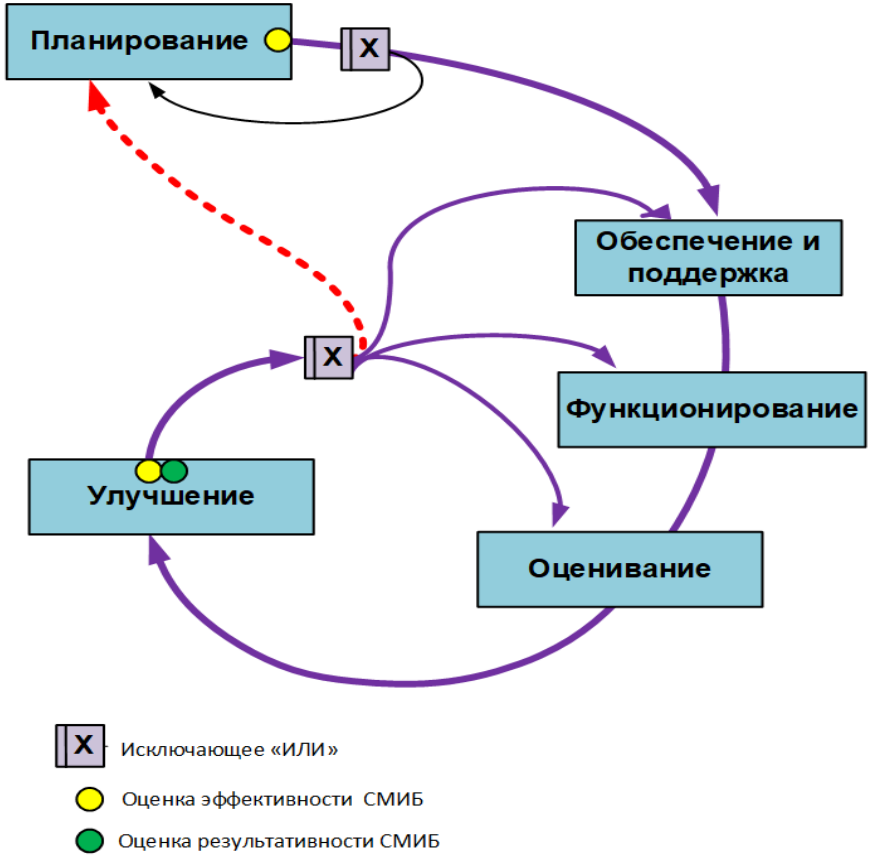
конференция РусКрипто

Оценка эффективности систем управления информационной безопасностью: проблемы и механизмы их решения.

- Минзов Анатолий Степанович, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ»
- Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ
- Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ

18.03.2025

ГОСТ Р ИСО/МЭК 27001-2021 г. Системы менеджмента информационной безопасности. Требования



Что мы понимаем под эффективностью СМИБ ?

Существует два типа показателей оценки выполнения запланированных действий в СМИБ[1]:

1. ***Показатели результативности,*** которые определяют степень выполнения планируемых мероприятий по обеспечению ИБ.

2. ***Показатели эффективности,*** отражающие влияние реализации запланированных мероприятий на цели ИБ организации. Основными показателем эффективности являются:

1. **Оценка возможного ущерба (*U*).**
2. **Сокращение затрат (Z) на устранение последствий инцидентов ИБ и восстановление *(U-Z)≥0*.**
3. **Обеспечение непрерывности критических процессов.**
4. **Ограничения на МИБ и другие показатели плана обработки рисков.**

[1] ГОСТ Р ИСО/МЭК 27004-2021. Информационные технологии. Мониторинг, оценка защищенности, анализ и оценивание

Модели управления рисками (*ISO-27005*)

$R = A \cap T \cap V$, $A \neq \varnothing, T \neq \varnothing, Y \neq \varnothing$;

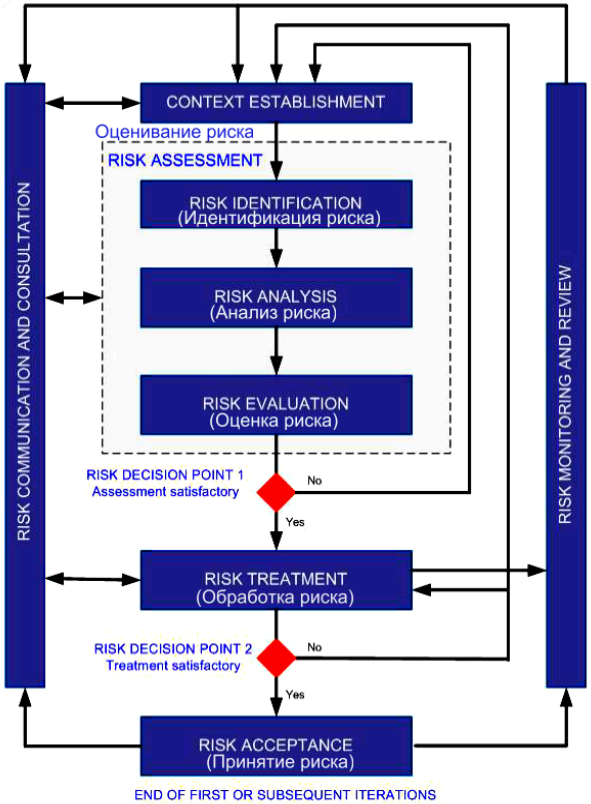
<*Nt, T, Na, A, Nv, V , M, Var, Mc, Z, [Ka]*>

где ***A,T,V*** – активы (оценка ценности), угрозы (оценка возможности) и уязвимости (оценка слабости);

Nt, Na, Nv, M – наименования (коды) угроз, активов, уязвимостей, метрика риска (относительные ед.);

$m_i = a_i + t_i + v_i$;

Var, Mc, Z, [Ka] – способ обработки риска, защитные контрмеры, затраты на обработку риска, коэфф. значимости актива.



Задачи, решаемые на этих моделях рисков (1,2)

1.Обоснование системы информационной безопасности на основе упорядочивания и классификации рисков (R) по степени опасности (K) и способу обработки рисков (S):

1.1. $\boldsymbol{R} = \{r_i\}$, *где* $r_i \geq r_{i+1} \geq r_{i+2} \geq \ldots \geq r_n$.

1.2 $\forall r_i, (r_i \in \boldsymbol{R}) \rightarrow (r_i \in \boldsymbol{K_1}) \cup (r_i \in \boldsymbol{K_2}) \cup (r_i \in \boldsymbol{K_3}) \ldots$,

где $\boldsymbol{K}$ *– класс опасности риска.*

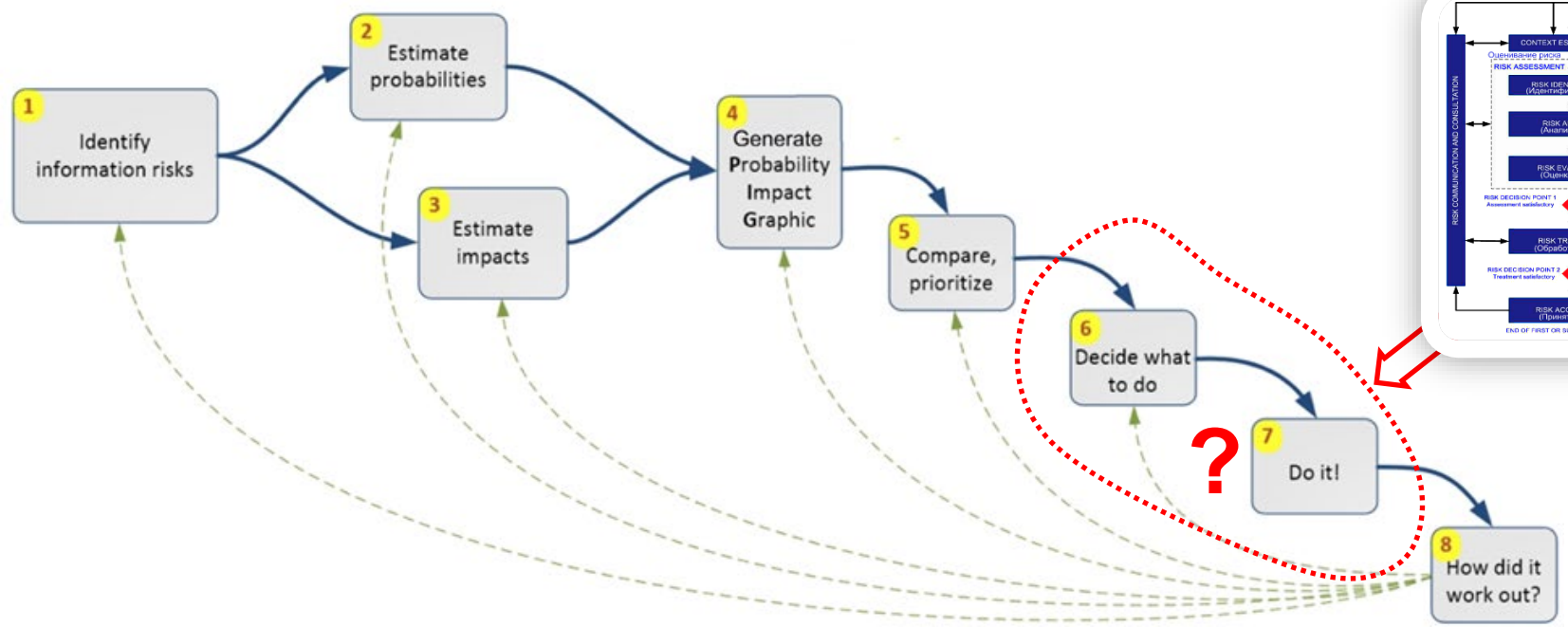
1.3. $\forall r_i, (r_i \in \boldsymbol{S}) \rightarrow (r_i \in \boldsymbol{S_1}) \cup (r_i \in \boldsymbol{S_2}) \cup (r_i \in \boldsymbol{S_3}) \cup (r_i \in \boldsymbol{S_4})$,

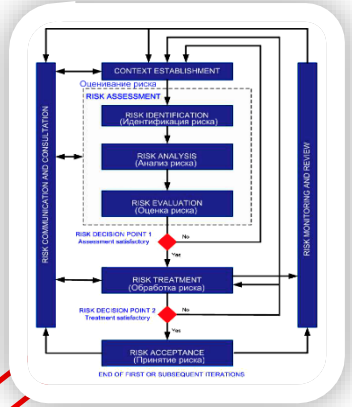
где $\boldsymbol{S_1}, \boldsymbol{S_2}, \boldsymbol{S_3}, \boldsymbol{S_4}$ *– способы обработки рисков: сохранение риска* ($\boldsymbol{S_1}$), *снижение риска* ($\boldsymbol{S_2}$), *перенос риска* ($\boldsymbol{S_3}$), *предотвращение риска* ($\boldsymbol{S_4}$).

?

Этого явно недостаточно, чтобы оценить корректность плана обработки рисков с позиций администрации организации.

Схема обработки рисков компании ITSEG (ENG)





Как оценивается эффективность СМИБ за рубежом?

1. **ISO 27001, 27005 (Европа).** Описан общий подход оценки оценки предполагаемого ущерба (U) на качественном уровне (ранжирования по шкалам).
2. **RiskWatch (США).** Основными оценочными показателями являются ожидаемые годовые потери и оценка возврата инвестиций.
3. **OCTAVE (США).** В методике OCTAVE оценивается только предполагаемый ущерб на количественном уровне (денежном эквиваленте ущерба) ‘экспертным путем.
4. **CORAS (США).** Качественная оценка рисков: предполагаемый ущерб инцидента и вероятность его возникновения.
5. **CRAMM** (Великобритания, с 1985 г.). Основная идея этой технологии управления заключается ***в накоплении практического опыта*** в форме шаблонов контрмер, активов, комбинаций ущербов, угроз, рисков, типовых политик и других документов.

Boehmer W. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001 //2008 Second International Conference on Emerging Security Information, Systems and Technologies. – IEEE, 2008. – С. 224-231.

Модели управления рисками для оценки эффективности плана обработки рисков

3. Параметрическая модель рисков

$R = (A \cap T \cap Y)$, где $A \neq \varnothing$, $T \neq \varnothing$, $Y \neq \varnothing$;

$<Nt, T, Na, A, Nv, V, M, U, Var, Mc, Z, [Ktv], sz, su, U\text{-}Z>$

4. Параметрическая модель рисков для умышленных угроз

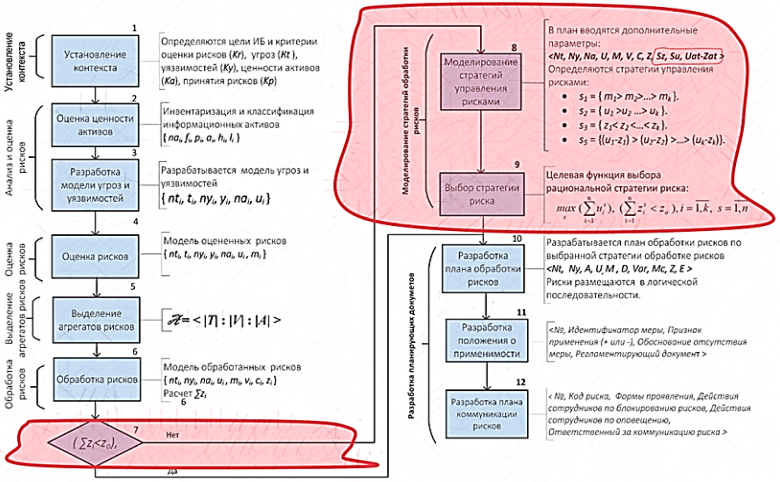
$R = (A \cap T)$, где $A \neq \varnothing$, $T \neq \varnothing$;

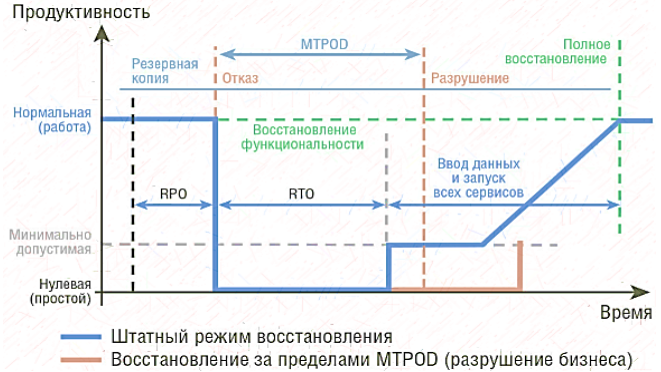
$< Nt, T, Na, A, U, M, Var, Mc, Zat, [Ktv], sz, su, U\text{-}Z >$

5.Параметрическая модель рисков при планировании непрерывности бизнес процессов

$R = (A \cap T \cap Y) \cup (A \cap T)$, где $A \neq \varnothing$, $T \neq \varnothing$, $Y \neq \varnothing$;

$< a_i , t_i , [v_i ,] r_i , \Delta t_i , \{c_{ij}\}, z_i >$





Критерии эффективности плана обработки рисков

1. План обработки рисков может быть ограничен по затратам z_0

$$Cd_1 = \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}.$$

2. План обработки рисков обеспечивает максимальную разницу между оценками возможного ущерба и затрат

$$Cd_2 = \max_s \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), i = \overline{i,k}, s = \overline{1,n}$$

3. Условно-оптимальный план обработки рисков при максимальном значении возможного ущерба и ограничениях на затраты

$$Cd_4 = \max_s \left(\sum_{i=1}^{k} u_i^s \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}.$$

Откуда взять количественные значения параметров возможного ущерба *U* ?

1. Непосредственно с использованием экспертных оценок по каждому риску.
2. С использованием метода нечетких множеств задаются параметры классификаций лингвистических переменных, их шкал измерения, форм функций принадлежности и определяются правила их взаимовлияния. Определяются значения *(U)* и определяются верхние и нижние границы полученных значений рисков.
3. Методом имитационного моделирования. С использованием качественного метода оценки параметров рисков в форме лингвистических переменных, переводом их в числовые значения и нахождением метрики рисков в относительных единицах ***m = t+a+v.*** Сумма метрик по каждому риску переводится из относительно значения денежную форме после нахождения удельного значение метрики m_d в тыс.руб. $m_d = z_m/(\Sigma m_i)$. ***Так определяется нижняя граница (U).***
4. Для определения ***верхней границы*** (U) задаются граничные количественные значения лингвистических переменных, проводится имитационное моделирование рисков и определяются погрешности моделирования среднего значения параметра предотвращенного ущерба.

Результаты моделирования параметров СМИБ на этапе ее проектирования

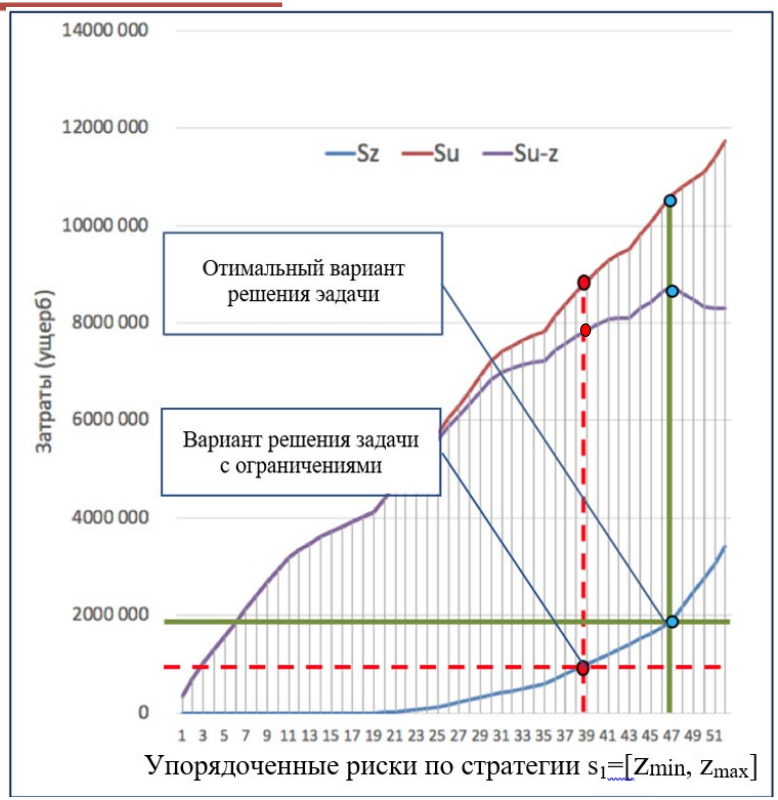


График определения показателей эффективности плана по критерию CD2 (оптимальный вариант) и CD3 (лучший вариант с ограничением по затратам)

ОГРАНИЧЕНИЯ

1.Оценка проводится только по умышленным рискам.

2. Допустимо соотношение $k \cdot \sum m_i \Leftrightarrow u_0$

3. $\forall m_i, (u_i \geq m_i)$

$$Cd_2 = \max_s \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), i = \overline{i,k}, s = \overline{1,n}$$

$$Cd_3 = \max_s \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}.$$

Заключение

1. Предложенные модели рисков позволяют расширить круг задач по управлению рисками информационной безопасности даже в отсутствии параметра неизвестной уязвимости. Это достигается за счет определения угроз для критичных активов.
2. На основе их анализа предложены механизмы оценки рисков (возможных ущербов) в относительных метриках измерений и методика перехода в абсолютные их значения в экономических показателях.
3. Такой подход позволяет проводить сравнительную оценку эффективности различных вариантов построения системы защиты информации, расширяя возможности требований нормативных документов регуляторов.

Вопросы !

Минзов Анатолий Степанович, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ» (MinzovAS@mpei.ru)

Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ

Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ