

Мистров Л.Е.

Метод оценки эффективности подсистем управления систем информационной безопасности

Аннотация: Рассматривается аналитический метод оценки эффективности подсистемы управления системы информационной безопасности по частным показателям оперативности и обоснованности принимаемых решений.

Ключевые слова: система информационной безопасности, подсистема управления, показатели оперативности и обоснованности решений

Введение

В современных условиях выполнение важных задач обеспечения безопасности организационно-технических систем (ОТС) осуществляется системами информационной безопасности (СИБ). Эффективность применения СИБ определяется планами, стратегиями и способами управления их ограниченными ресурсами. Управление СИБ представляет целенаправленный процесс преобразования исходной информации для выработки управляющей (распорядительной) информации с целью ее перевода в требуемое состояние.

Процесс управления СИБ носит информационный характер и представляется в виде совокупности различных процедур (операций) по поиску, сбору, обработке и преобразованию информации ее подсистемой управления (рассматриваемой в виде системы управления – СУ) для выработки управляющих воздействий и доведения их до объектов управления (СИБ в целом, ее элементов) с контролем эффективности исполнения. Критерием оценки эффективности СУ является множественность показателей эффективности (ПЭ), характеризующих результаты деятельности СИБ.

Оценку эффективности СУ возможно осуществлять по ПЭ на уровне СИБ или на уровне ее подсистемы управления, обобщенно объединенных в две взаимосвязанные группы показателей:

на уровне СИБ – эффективность СУ характеризуется интегральными результатами деятельности СИБ в виде получаемой прибыли ОТС, себестоимости и т.п., в том числе и затрат на мероприятия по управлению (при этом вклад СУ в результаты деятельности СИБ трудно выделить);

на уровне СУ – эффективность характеризуется ПЭ, отражающих содержание и организацию процесса управления СИБ и характеризующих производительность, своевременность, оперативность, гибкость и достоверность управляющих решений.

Перечисленные ПЭ основных свойств СУ носят нормативный характер и могут использоваться в качестве критериев эффективности ее функционирования. Основным требованием к ним является чувствительность к основным внешнесистемным и внутрисистемным характеристикам условий и способов конкурентного взаимодействия ОТС. В виду возможной реализации конкурирующими ОТС способов взаимодействия на основе формирования активных (преднамеренно создаваемых) и пассивных (вследствие негативных погодных условий и непреднамеренно создаваемых) информационных воздействий на СУ объем информации, поступающей лицам, принимающим решение (ЛПР), снижается, обуславливая возникновение информационных потерь в структуре ее контуров принятия решений. Вследствие этого, объем информации становится меньше необходимого для выработки СУ управляющих воздействий, что приводит к соответствующему изменению ПЭ принимаемых решений.

Определение ПЭ СУ может осуществляться исходя из наличия информации об условиях конфликтного взаимодействия ОТС с использованием методов математического моделирования. Необходимость учета факторов неопределенности о состоянии, структуре и характеристиках ОТС на множестве способов их активного / пассивного конфликтного взаимодействия и установления причинно-следственных связей между ПЭ управления и информационными потерями в контурах принятия решений СУ затрудняет оценить ее вклад в эффективность СИБ. Данное противоречие обуславливает разработку математических моделей для оценки по частным ПЭ ее применения, что определило цель и содержание представленной работы.

1. Модель оценки оперативности принятия решений ЛПР

Оперативность управления является определяющим свойством СУ, характеризующим ее способность вырабатывать решения в установленные сроки. Она является функцией длительности составляющих операций выработки решения и его доведения до объектов управления (ОУ). Поэтому любые действия, направленные на снижение эффективности СУ, приводят к увеличению продолжительности процесса принятия решения (ПР). Оценка оперативности управления производится на основе минимизации длительности принятия решения СУ в виде:

$$T_{СУ} = \min_t (t_{np} + t_{дов}) \leq T_{оц}, \quad (1)$$

где $T_{оц}$ – среднее время анализа исходной информации ЛПР для ПР на множестве характеристик воздействия внешней среды; t_{np} – время ПР; $t_{дов}$ – время доведения ЛПР управляющих воздействий до ОУ.

Все составляющие в (1) характеризуются математическим ожиданием, определяемым длительностью операций по работе с информацией ЛПР.

Наиболее полной характеристикой своевременности ПР СУ, в отличие от показателя длительности управления (1), является коэффициент оперативности, определяемый в виде:

$$K_{он} = \max_t [P(T_{СУ} \leq T_{оц})] = \max_t [1 - P(T_{СУ} \geq T_{оц})], \quad (2)$$

где $P(T_{СУ} \geq T_{оц})$ – вероятность превышения продолжительности ПР СУ времени оперативной ценности информации (риск несвоевременного ПР).

В предположении нормального закона распределения продолжительности процесса ПР СУ, характеризуемого длительностью управленческих действий ЛПР с математическим ожиданием $T_{СУ}$ и дисперсией $\sigma_{СУ}$, вероятность несвоевременного принятия решения будет равна:

$$P(T_{CY} \geq T_{OY}) = \frac{1}{\sqrt{2\pi}} \int_{T_{OY} - T_{CY} / \sigma_{CY}}^{\infty} e^{-\frac{t^2}{2}} dt = \Phi \left[\frac{T_{OY} - T_{CY}}{\sigma_{CY}} \right], \quad (3)$$

где $\Phi = [(T_{OY} - T_{CY}) / \sigma_{CY}]$ – табулированная функция нормального распределения.

Вероятность (3) фактически характеризует риск несвоевременного ПР $P(T_{CY} \leq T_{OY}) = 1 - P(T_{CY} \geq T_{OY})$, который тем больше, чем меньше параметр Δ . Параметр же $\Delta = (T_{OY} - T_{CY}) / \sigma_{CY}$ в (3) при выполнении условия $P(T_{CY} \geq T_{OY}) = const$ определяет требования к продолжительности ПР СУ как функции характеристик условий способов конфликтного взаимодействия ОТС, объема и качества информации, а также слаженности работы ее ЛПР при выработке решения. На рисунке 1 приведена зависимость параметра Δ от возможного значения риска несвоевременного ПР, а на рисунке 2 – зависимость коэффициента оперативности управления (2) от параметра Δ , характеризующего возможность (как следует из рисунка 1) технического и информационного обеспечения и слаженность работы ЛПР при ПР.

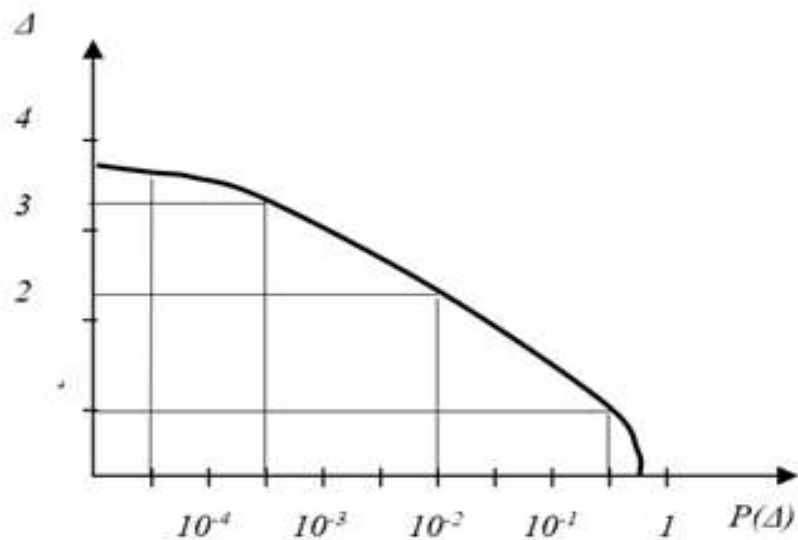


Рисунок 1 – Зависимость требований к продолжительности управления от риска несвоевременного ПР

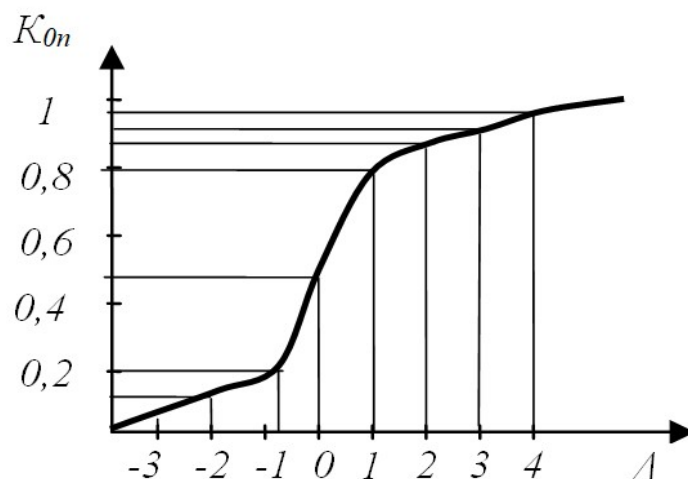


Рисунок 2 – Зависимость показателя оперативности управления от подготовленности ЛПР качественно ПР

В общем случае, риск несвоевременного ПР должен быть минимально возможным, и равен, как следует из зависимости на рисунке 1, например, $P(T_{CY} < T_{ou}) = 10^{-2} - 10^3$, то есть подготовленность ЛПР, определяемая параметром Δ , должна удовлетворять условию:

$$\Delta = (T_{ou} - T_{CY}) / \sigma_{CY} \geq 2, \dots, 3. \quad (4)$$

При выполнении условия (4), как следует из рисунка 2, $K_{on} \cong 1$ применительно к условиям функционирования СУ при наличии необходимой информации для ПР. Исходя из этого, разница между временем анализа ценности информации и средним временем, необходимым для ПР, должна составлять не менее трех среднеквадратических отклонений (СКО) продолжительности подготовки решения ЛПР, принятия его и доведения до ОУ. Это означает, что информация передается на СУ с заданной достоверностью, достаточной для принятия эффективного решения.

2. Модель оценки обоснованности принятия решения ЛПР

Обоснованность ПР по управлению СИБ определяется способностью ее СУ преобразовывать исходную информацию в управляющую информацию для обеспечения перехода ОУ из текущего в требуемое состояние, соответствующее сложившейся

обстановке. В этом случае, в качестве показателя обоснованности используется вероятность (коэффициент), определяющая риск принятия СУ неэффективного решения $p_p = K_{нпр}$ как функции неопределенности исходной информации о состоянии СИБ, характеристиках условий конкурентного взаимодействия ОТС, а также качества используемого в процессе ПР методического обеспечения.

Одним из путей учета влияния неопределенности и неполноты исходной информации на обоснованность решений СУ является проведение анализа числа вариантов решений и их сравнение с числом (M_0) вариантов, которые могли бы быть рассмотрены при наличии необходимой информации. В этом случае временные ресурсные возможности СУ являются ограниченными, вследствие чего имеется возможность рассмотрения только m вариантов решений ($m \leq M_0$). Это особенно характерно на этапе оперативного управления, когда решения СУ базируются на информации о характеристиках внешней среды и состоянии ОТС.

В общем случае, определение коэффициента риска принятия СУ неэффективного решения осуществляется на основе соотношения [1]:

$$K_{нпр} = \min_{T_p, \Delta T_p} \left(1 - \frac{m}{M_0} \cdot \varphi_m \right), \quad (5)$$

где $m = T_p / \Delta T_p$ – число вариантов, которое может рассмотреть СУ за отведенное время (T_p) на ПР при ΔT_p времени на решение одного варианта;

φ_m – коэффициент качества методического аппарата и слаженности работы ЛПР СУ ($0 \leq \varphi_m \leq 1$).

В модели (5) конкретные значения M_0 и φ_m определяются исходя из содержания и особенностей решаемой задачи с учетом обеспеченности ЛПР необходимой исходной информацией о характеристиках условий способов конфликтного взаимодействия ОТС.

А. В общем случае оперативность принятия решений СУ определяется средней длительностью T_{cy} , которая в условиях активного воздействия внешней конкурентной среды на СУ (в частности, ее каналы связи) и при наличии хотя бы в одной из линий радиосвязи (ЛРС) γ уровня информационного ущерба рассчитывается в виде:

$$T_{CY}^* = T_{CY} + \xi(\gamma) \cdot T_c, \quad (6a)$$

где $\xi(\gamma)$ – относительное время задержки (число повторений) сообщения длительностью T_c при наличии информационного ущерба на уровне γ .

При условии обеспечения процесса ПР СУ системой радиосвязи (СРС) в составе нескольких ЛРС (N), в том числе и разнородных, при снижении эффективности нескольких ЛРС на уровне γ оперативность ПР СУ (6a) преобразуется к виду:

$$T_{CY}^{*CPC} = T_{CY} + \sum_{n=1}^N \varepsilon_n \xi_n(\gamma) \cdot T_{cn}, \quad \varepsilon_n < 1, \quad \sum_{n=1}^N \varepsilon_n = 1, \quad (6b)$$

где ε_n – весовой коэффициент, характеризующий влияние поступающей по n -й ЛРС информации на увеличение продолжительности процесса ПР СУ;

$\xi(\gamma)$ – относительное время задержки информации, определяемое соотношением [2]:

$$\xi(\gamma) = \frac{\ln P_{ош}^{don}}{\ln \gamma} - 1; \quad (7)$$

где $P_{ош}^{don}$ – допустимая вероятность ошибки, определяемая требуемой достоверностью передачи управляющей информации.

При активном информационном воздействии конкурирующей СИБ на каналы передачи информации (КПИ) СРС СУ определение вероятности несвоевременного ПР осуществляется в виде [2]:

$$P(T_{oy} > T_{ou}) = \Phi \left[-\Delta_0 \left(1 - \frac{\sum_{n=1}^N \varepsilon_n \xi_n T_{cn}}{\Delta_0 \sigma_{oy}} \right) \right] = \Phi \left[-\Delta_0 \left(1 - \frac{1}{\Delta_0 \sigma_{oy}} \sum_{n=1}^N \varepsilon_n T_{cn} \cdot \frac{\ln P_{ou}^{(\partial on)}}{\ln \gamma} \right) \right], \quad (8)$$

где $\Phi(\cdot)$ – функция нормального распределения; Δ_0 – параметр, определяющий подготовленность ЛПР СУ к работе в отсутствие воздействия внешней среды.

Как следует из (8), риск принятия несвоевременного ПР СУ возрастает с увеличением информационного ущерба (времени задержки информации).

При принятии относительного риска несвоевременного ПР СУ в качестве показателя оперативности управления используется коэффициент оперативности ПР, значение которого может определяться в виде:

$$\bar{K}_{oy} = \frac{P(T_{oy} > T_{ou}, \xi)}{P(T_{oy} > T_{ou}, \xi = 0)} = \frac{\Phi \left[-\Delta_0 \left(1 - \frac{1}{\Delta_0 \sigma_{oy}} \cdot \sum_{n=1}^N \varepsilon_n \xi_n T_{cn} \right) \right]}{\Phi(-\Delta_0)}. \quad (9)$$

При $\Delta_0 \gg 1$, учитывая асимптотическое представление интеграла вероятности $\Phi(x) \cong 1 - 1/(2\sqrt{\pi x})e^{-x^2}$, $x \gg 1$, представим показатель (9) при $\sum_{n=1}^N \xi_n \varepsilon_n T_{cn} < \sigma_{oy} \Delta_0$ в виде:

$$\bar{K}_{oy} \cong \exp \left\{ - \left[\sum_{n=1}^N \varepsilon_n \xi_n b_n \right] \right\}, \quad (10)$$

где $b_n = T_{cn} / \sigma_{oy}$ – отношение длительности передаваемого по n -й ЛРС сообщения к СКО продолжительности принятия решения.

Для случая, когда $N=1$ и $\Delta_0=3$, на рисунке 3 приведено семейство зависимостей показателя риска несвоевременного принятия решения в виде (9) от времени задержки информации, нормированной к СКО продолжительности процесса принятия

решения СУ в отсутствие активного воздействия конкурирующей СИБ на ЛРС. На рисунке 4 приведено семейство зависимостей показателя оперативности управления (8) от переменной, определяемой информационным ущербом (γ), связанным со временем задержки информации соотношением (7).

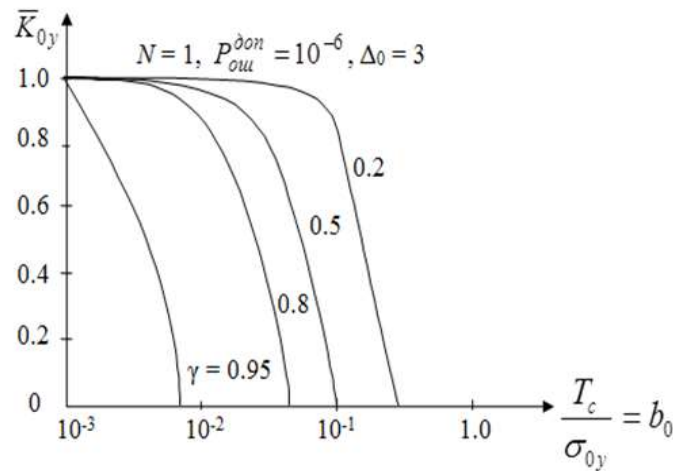


Рисунок 3 – Изменение показателя от относительного времени задержки информации при передаче по ЛРС

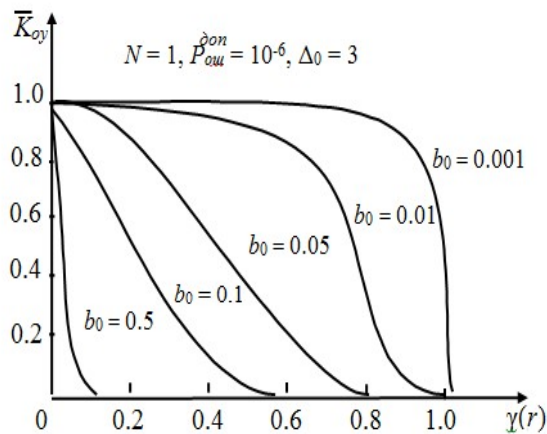


Рисунок 4 – Зависимость показателя от уровня ущерба ЛРС при передаче информации

Анализ приведенных на рисунках 3 и 4 зависимостей позволяет сделать следующие выводы.

1. На показатель оперативности управления, в условиях активного воздействия конкурирующей ОТС, существенное влияние оказывает отношение длительности передаваемого по ЛРС

сообщения (T_c) к СКО продолжительности принятия решения (σ_{oy}). Численное значение σ_{oy}^2 зависит как от числа принимаемых вариантов решений, состояния информационно-методического обеспечения и слаженности работы ЛПР СУ.

2. Для одной и той же СУ ($\sigma_{oy}^2 = \text{const}$), при одном и том же количестве информации для ПР, показатель оперативности управления зависит от относительной длительности сообщения (T_c / σ_{oy}). Чем больше длительность сообщения, тем больше требуется времени для получения всего количества информации с требуемой достоверностью ($P_{ош} = 10^{-6}$), а это приводит к соответствующему снижению показателя оперативности управления (рисунок 5).

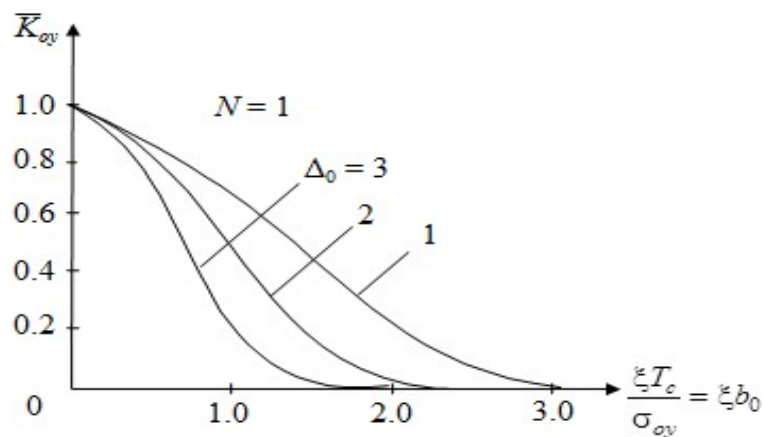


Рисунок 5 – Зависимость влияния длительности сообщения, передаваемого в условиях активного воздействия конкурирующей ОТС на показатель оперативности СУ

Б. Для принятия СУ оптимального решения требуется проведение анализа большого количество вариантов решений. Вследствие того, что временные ресурсные возможности СУ ограничены, то ПР осуществляется исходя из возможности рассмотрения только M_0 ограниченного числа вариантов. Число M_0 вариантов зависит от отведенного времени (T_p) на ПР решения и среднего времени (ΔT_0) на решение одного варианта в виде:

$$M_0 = T_p / \Delta T_0 \quad \text{при } T_p < T_{\text{от}}. \quad (11)$$

Таким образом, T_p время на ПР СУ (как следует из анализа (11)) должно быть меньше времени оперативной ценности информации, а качество используемого в процессе ПР методического аппарата и информационной базы данных может определяться некоторым параметром $\varphi_m \leq 1$, значение которого устанавливается исходя из анализа качества применяемого СУ технического и информационно-методического обеспечения.

В заключение следует отметить, что эффективность СУ возможно оценивать по интегральному показателю применения СИБ или совокупности частных показателей, основными из которых являются своевременность, оперативность и обоснованность (достоверность) принятых управленческих решений. Определение частных показателей эффективности СУ базируется на использовании аналитических и информационных моделей, позволяющих оценить:

оперативность принятия решений СУ на основе определения коэффициента оперативности, рассчитываемого на основе центральной теоремы вероятностей;

обоснованность принимаемых решений по вероятности (коэффициенту), определяющей риск принятия некачественного решения, обусловленного активным воздействием конкурирующей ОТС на СУ. На оперативность управления существенное влияние оказывает длительность передаваемого сообщения (распорядительной информации) и среднеквадратического отклонения продолжительности принятия решения;

достоверность принятого решения, определяемого наличием в СУ информационного ресурса и помехозащищенностью системы радиосвязи органа управления ОТС. Принятие решений СУ основывается на анализе альтернативных вариантов решений и выборе предпочтительного как функции показателя достоверности от количества рассмотренных вариантов решений.

Литература:

1. Основы теории управления в системах военного назначения. Ч. 2. Учебное пособие / Под. ред. А.Ю. Руднего и И.В. Котенко. – СПб.: ВУС, 2000 – 158 с.

2. *Владимиров В.И.* Информационные основы радиоподавления линий радиосвязи в динамике радиоэлектронного конфликта. – Воронеж: ВИРЭ, 2003. – 276 с.

DOI: 10.25728/iccss.2023.84.45.030

Муромцева А.В., Муромцев В.В., Кузнецов Д.В.

Информационные угрозы виртуального пространства

Аннотация: Информационное виртуальное пространство сегодня активно используется для реализации различных информационных технологий. Появляются и новые угрозы информационной безопасности. Конкретным примерам подобных угроз и посвящена работа.

Ключевые слова: виртуальное информационное пространство, угрозы информационной безопасности, информационные сайты, OpenStreetMap, информационное противостояние

В современном виртуальном информационном пространстве, кроме социальных сетей, которые позволяют людям общаться, делиться информацией и виртуально взаимодействовать друг с другом, имеются информационные сайты, содержащие разнообразную информацию, обеспечивающие потребности различных пользователей. Помимо очевидных плюсов удаленной коммуникации есть ряд скрытых угроз, которые они в себе таят.

Современное виртуальное информационное пространство стало глобальным. Это привело к существенным изменениям во всех сферах деятельности человека: технической, технологической, культурной, социальной, политической, экономической. Появились и новые угрозы информационной безопасности.

В информационном пространстве активно используются программные продукты, которые требуются для решения множества производственных задач. Эти программные продукты находятся в общем доступе и их принадлежность различная. Есть платные информационные сайты, условно платные и сайты, получение информации с которых не требует денежных затрат. Примерами являются такие системы как Википедия, OpenStreetMap