

*Шабурова Аэлита Владимировна, д.э.н., доцент, директор Института оптики и технологий информационной безопасности*  
*Обиденко Антон Владимирович, магистрант*  
*Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет геосистем и технологий» (СГУГиТ), Россия, 630108, г. Новосибирск, ул. Плеханова, дом 10.*

## **МОДЕЛИРОВАНИЕ ВЛИЯНИЯ АРХИТЕКТУРЫ СЗИ НА ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС**

**Аннотация.** В статье решается задача выбора архитектуры системы защиты информации (СЗИ) для образовательной организации на основе количественного критерия доступности. В качестве такого критерия используется интегральный коэффициент доступности образовательной среды ( $A$ ), используемый ранее. Путем аналитического моделирования проанализировано влияние пяти типовых архитектур развертывания межсетевых экранов (одиночный, каскадный, с балансировкой нагрузки, сегментированная сеть, схема «сэндвич» с DMZ) на ключевые составляющие коэффициента  $A$ : стабильность сети и уровень ложных блокировок. На основе единых исходных данных проведен сравнительный расчет итоговых значений коэффициента  $A$  для каждой архитектуры. Установлено, что схема с балансировкой нагрузки обеспечивает максимальное значение доступности ( $A=0,985$ ), в то время как каскадная схема и схема «сэндвич» приводят к ее значительному снижению ( $A<0,93$ ). Полученные результаты позволяют обосновать рекомендации по построению СЗИ, оптимальной с точки зрения компромисса между безопасностью и непрерывностью учебного процесса.

**Ключевые слова:** архитектура системы защиты информации, межсетевой экран, доступность, коэффициент доступности, моделирование, образовательная организация, балансировка нагрузки.

## **Введение**

Внедрение современных систем защиты информации (СЗИ) в образовательных организациях сопряжено с необходимостью выбора архитектурных решений, которые определяют не только уровень защищенности, но и эксплуатационные характеристики инфраструктуры. Традиционно при проектировании СЗИ фокус смещен в сторону максимизации безопасности, что зачастую приводит к реализации сложных, многоуровневых схем (каскадирование, изоляция сегментов) [1, 2]. Однако такие схемы могут негативно влиять на доступность информационных сервисов за счет введения дополнительных точек отказа и увеличения вероятности ложных блокировок легитимного трафика [3]. Для образовательного процесса, где критически важна непрерывность работы электронных обучающих систем и сетевых ресурсов, данное влияние неприемлемо.

В предыдущей работе авторами был предложен интегральный коэффициент доступности образовательной среды (А) как инструмент количественной оценки воздействия СЗИ на учебный процесс [4]. Целью настоящего исследования является применение данного коэффициента для сравнительного анализа и выбора оптимальной архитектуры СЗИ, обеспечивающей баланс между безопасностью и доступностью. Для этого проводится аналитическое моделирование пяти типовых архитектурных решений, а сам подход к сравнительной оценке соответствует современной практике многокритериального анализа в ИБ [5].

## **1. Методология и исходные данные моделирования**

В основе методологии лежит расчет коэффициента  $A$  для различных архитектур и является взвешенной суммой четырех частных показателей:

$$A = \sum_{j=1}^m w_j A_j \quad (1)$$

Поскольку выбор архитектуры СЗИ в наибольшей степени влияет на стабильность сети ( $A_2$ ) и уровень ложных блокировок ( $A_3$ ), в рамках данного моделирования значения  $A_1$  (доступность сервисов) и  $A_4$  (аутентификация) приняты условно постоянными и высокими:  $A_1 = 0,995$ ,  $A_4 = 0,995$ . Веса критериев используются полученные ранее методом анализа иерархий:  $w_1=0,28$ ,  $w_2=0,47$ ,  $w_3=0,16$ ,  $w_4=0,09$  [4].

#### **Базовые параметры для моделирования едины для всех архитектур:**

- Надежность одного экземпляра межсетевого экрана (МЭ):  $A_{2(\text{МЭ})} = 0,995$  (коэффициент готовности).
- Вероятность ложного срабатывания одного МЭ:  $P_{false} = 0,05$  (5%).
- Логика взаимодействия МЭ в архитектуре (последовательная, параллельная) определяет итоговые  $A_2$  и  $A_3$ . [6]

Рассматриваются следующие пять архитектур (Рис. 1):

1. **Архитектура 1 («Одиночный МЭ»):** Один межсетевой экран на границе сети.
2. **Архитектура 2 («Каскадная»):** Два различных МЭ, подключенных последовательно. Трафик проходит проверку поочередно в каждом.
3. **Архитектура 3 («Балансировка нагрузки»):** Два однотипных МЭ, работающих параллельно в режиме активный-активный. Трафик распределяется между ними, отказ одного не приводит к остановке системы.
4. **Архитектура 4 («Сегментированная сеть»):** Внутренняя сеть разделена на изолированные сегменты

(студенты/преподаватели/администрация) с собственными МЭ между ними. Для оценки рассматривается доступность сквозного соединения между сегментами.

5. **Архитектура 5 («Сэндвич», DMZ):** Публичные сервисы размещены в демилитаризованной зоне (DMZ), окруженной двумя МЭ (внешним и внутренним).

## 2. Результаты сравнительного моделирования

Для каждой архитектуры выполнены расчеты итоговых показателей  $A_2$  и  $A_3$  с учетом логики их построения. Результаты сведены в Таблицу 1.

**Таблица 1. Влияние архитектуры СЗИ на показатели доступности**

Архитектура	Логика взаимодействия	Расчет $A_2$ (стабильность)	Расчет $A_3$ (ложные блокировки)	Итоговый А
1. Одиночный МЭ	Один элемент	$A_2 = 0,995$	$A_3 = 1 - 0,05 = 0,95$	0,978
2. Каскадная	Последовательное соединение	$A_2 = 0,995 \times 0,995 \approx 0,990$	$A_3 = 1 - (0,05 + 0,05 - 0,05 \times 0,05) = 0,9025$	0,926
3. Балансировка	Параллельное соединение	$A_2 = 1 - (1 - 0,995)^2 \approx 0,999975$	$A_3 = 1 - (0,05 \times 0,05) = 0,9975$	0,985
4. Сегментированная	Последовательная для	$A_2 = 0,990$ (как в каскаде)	$A_3 = 0,90$ (повыш.)	0,945

Архитектура	Логика взаимодействия	Расчет $A_2$ (стабильность)	Расчет $A_3$ (ложные блокировки)	Итоговый $A$
	межсегм. трафика		риск внутр. блок.)	
5. «Сэндвич» (DMZ)	Последоват. для доступа внутрь	$A_2 = 0,990$	$A_3 = 0,9025$ (как в каскаде)	0,915

- **Последовательное соединение (арх. 2,4,5):** Система отказывает, если откажет любой элемент. Надежность перемножается:  $A_{2(сист)} = A_{2(МЭ)}^n$ . Ложная блокировка происходит, если работает любой МЭ:

$$A_{3(сист)} = 1 - (1 - (1 - P_{false})^n) \quad (2)$$

- **Параллельное соединение (арх. 3):** Система отказывает, только если откажут все элементы.

$$A_{2(сист)} = 1 - (1 - A_{2(МЭ)}^n) \quad (3)$$

- Ложная блокировка происходит, только если сработают все МЭ одновременно:

$$A_{3(сист)} = 1 - P_{false}^n \quad (4)$$

- Итоговый коэффициент  $A$  рассчитан по формуле (1) с учетом постоянных  $A_1$  и  $A_4$ .

### 3. Результаты

Проведенное моделирование выявило значительный разброс значений коэффициента доступности  $A$  в зависимости от выбранной архитектуры СЗИ (от 0,915 до 0,985). Это наглядно демонстрирует, что архитектурный выбор

является критическим фактором для обеспечения непрерывности учебного процесса.

1. Наихудшие результаты показали архитектуры, основанные на последовательном соединении элементов защиты: каскадная ( $A=0,926$ ) и «сэндвич» ( $A=0,915$ ). Несмотря на потенциально высокий уровень безопасности (многоуровневая проверка), они неприемлемы для образовательной среды из-за мультипликативного эффекта ложных блокировок и снижения общей надежности. Их значение  $A$  находится в «неприемлемой» зоне ( $A < 0,970$ ).
2. Сегментированная архитектура ( $A=0,945$ ) занимает промежуточное положение. Она обеспечивает высокую безопасность за счет изоляции сегментов, но также негативно влияет на доступность для легитимного межсегментного взаимодействия, необходимого в учебном процессе.
3. Оптимальный результат продемонстрировала архитектура с балансировкой нагрузки ( $A=0,985$ ). Благодаря параллельной работе МЭ она обеспечивает:
  - **Максимальную отказоустойчивость** (почти идеальная надежность  $A_2$ ).
  - **Минимальный риск ложных блокировок** (требуется одновременное срабатывание обоих МЭ).
  - **Высокое значение интегрального коэффициента  $A$** , соответствующее уровню «отличной доступности».

Таким образом, для типовой образовательной организации, где приоритетом является сочетание достаточной безопасности и высокой доступности, архитектура с балансировкой нагрузки является предпочтительной. Каскадные схемы и схемы с DMZ могут быть оправданы только для защиты изолированных, критически важных систем, не участвующих в ежедневном учебном процессе.

## **Заключение**

В работе на основе метода аналитического моделирования проведен сравнительный анализ влияния пяти типовых архитектур СЗИ на доступность образовательных сервисов. В качестве инструмента оценки использован ранее разработанный интегральный коэффициент доступности  $A$ .

Установлено, что архитектуры, основанные на последовательном соединении средств защиты (каскадная, «сэндвич»), приводят к неприемлемому снижению доступности ( $A < 0,93$ ) для образовательной среды из-за кумулятивного эффекта ложных срабатываний и низкой отказоустойчивости. Сегментированная сеть, обеспечивая высокую безопасность, также создает существенные ограничения на доступность ( $A=0,945$ ).

Архитектура с балансировкой нагрузки двух межсетевых экранов показала наилучший результат ( $A=0,985$ ), обеспечивая как высокую отказоустойчивость, так и минимальное вмешательство в легитимный трафик. Данная архитектура рекомендуется в качестве базовой для построения СЗИ в образовательных организациях, где непрерывность учебного процесса является ключевым требованием.

Полученные результаты подтверждают практическую ценность коэффициента  $A$  в качестве критерия для обоснованного выбора архитектурных решений при проектировании систем защиты информации.

## **Библиографический список**

1. Захаров А.Г., Москвитин Г.И. Архитектура корпоративных систем защиты информации // Информационные технологии и безопасность. – 2020. – № 4(12). – С. 45-56.
2. Тараскин М.М. Современные подходы к построению систем межсетевого экранирования // Вопросы кибербезопасности. – 2021. – № 3(42). – С. 32-40.

3. Калмуратова С.М. Анализ методов и методика оценки эффективности систем защиты информации // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 450-458.
4. Шабурова А.В., Обиденко А.В. Разработка методики оценки воздействия системы защиты информации на непрерывность учебного процесса // Прикладная информатика и вопросы кибербезопасности (статья принята к публикации). – 2024.
5. Иванов Р.С., Смирнова Л.К. Методы сравнения и выбора архитектурных решений в информационной безопасности на основе многокритериального анализа // Системный администратор. – 2023. – № 5(234). – С. 88-95.
6. Волков Д.Ю., Кравченко И.А. Оценка отказоустойчивости сетевых архитектур с учетом надежности межсетевых экранов // Надежность. – 2022. – Т. 22, № 4. – С. 67-74.