УДК 004.056.53

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. Плахотного, дом 10.

МЕТОДИКА ОЦЕНКИ ВОЗДЕЙСТВИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС

Аннотация. В статье рассматривается проблема оценки эффективности систем защиты информации (СЗИ) в образовательных организациях. Отмечается, что традиционные подходы, фокусирующиеся на технических показателях защищенности, не учитывают влияние СЗИ на доступность и непрерывность основного бизнес-процесса — учебной деятельности. С целью решения данной проблемы предложена новая методика, основанная на расчете интегрального коэффициента доступности образовательной среды (А). Коэффициент А представляет собой взвешенную сумму четырех частных показателей: доступности критических сервисов, стабильности сетевой инфраструктуры, уровня ложных блокировок и удобства аутентификации. Веса критериев определены с применением метода анализа иерархий Т. Саати. Приведен пример применения методики для моделирования условий вуза с контингентом в 7500 пользователей. Показано, что методика позволяет количественно оценить компромисс между безопасностью и доступностью, предоставляя инструмент для обоснования управленческих решений в области ИБ.

Ключевые слова: информационная безопасность, система защиты информации, доступность, образовательная среда, коэффициент доступности, оценка эффективности, метод анализа иерархий.

Введение

Цифровая трансформация образования, сопровождающаяся массовым внедрением электронных образовательных сред, систем дистанционного обучения и облачных сервисов, привела к значительному увеличению поверхности атаки информационной инфраструктуры вузов [1]. По данным Роскомнадзора, объем утечек персональных данных в России к 2025 году достиг 13 млрд записей, при этом образовательные организации, обрабатывающие данные студентов и сотрудников, являются одной из уязвимых групп [2]. Традиционно оценка эффективности СЗИ фокусируется на технических параметрах: вероятности обнаружения угроз, времени реакции, коэффициенте ложных срабатываний [3, 4]. Однако такой подход не учитывает ключевой аспект: любое средство защиты, внедряемое в рабочую инфраструктуру, оказывает прямое влияние на доступность информационных сервисов для конечных пользователей — преподавателей и студентов. Ложные блокировки легитимного учебного трафика, задержки из-за фильтрации, простои во время обновления или настройки средств защиты напрямую снижают качество образовательного процесса.

Таким образом, возникает проблема необходимости оценки не только собственно защищенности, но и операционного воздействия СЗИ на основную деятельность организации. Целью данной работы является разработка методики количественной оценки этого воздействия на основе интегрального коэффициента доступности образовательной среды.

1. Материалы и методы

Объектом исследования выступила информационно-телекоммуникационная инфраструктура и СЗИ образовательной организации. В качестве базового примера рассматривается вуз с контингентом около 7500 пользователей (7000 студентов и 500 сотрудников).

1.1. Формализация критериев доступности

Были формализованы четыре ключевых критерия, комплексно описывающих доступность образовательной среды с точки зрения пользователя:

1. **A_1 – Доступность критических образовательных сервисов.** Показывает долю времени, в течение которого ключевые системы (LMS, электронная почта, библиотечные ресурсы) доступны для работы.

$$A_1 = \frac{t_{общ} - t_{простоя}}{t_{общ}} \quad (1)$$

где $t_{общ}$ – общее рассматриваемое время, $t_{простоя}$ – суммарное время недоступности сервисов.

2. **A_2 – Стабильность сетевой инфраструктуры.** Характеризует надежность каналов связи и сетевого оборудования. Выражается через классические показатели теории надежности.

$$A_2 = 1 - \frac{MTTR_{сети}}{MTTF_{сети} + MTTR_{сети}} \quad (2)$$

где $MTTF_{сети}$ – средняя наработка на отказ, $MTTR_{сети}$ – среднее время восстановления.

3. **A_3 – Уровень ложных блокировок.** Отражает влияние СЗИ на легитимную учебную активность.

$$A_3 = 1 - \left(\frac{C_{ложных}}{C_{общее}}\right) \quad (3)$$

где $C_{ложных}$ – количество ошибочно заблокированных обращений к ресурсам, $C_{общее}$ – общее количество обращений.

4. **A_4 – Доступность и удобство аутентификации.** Учитывает проблемы пользователей при доступе к системам.

$$A_4 = 1 - \left(\frac{U_{жалоб}}{U_{общее}}\right) \quad (4)$$

где $U_{жалоб}$ – количество пользователей, сообщивших о проблемах с входом, $U_{общее}$ – общее число пользователей.

1.2. Интегральный коэффициент доступности (A)

Для получения общей оценки введен интегральный коэффициент доступности образовательной среды A, представляющий собой взвешенную сумму частных показателей:

$$A = \sum_{j=1}^{m} w_j A_j \qquad (5)$$

при условии:

$$\sum_{j=1}^{m} w_j = 1 \qquad (6)$$

Весовые коэффициенты w_j отражают относительную важность каждого критерия для конкретной организации.

1.3. Определение весов методом анализа иерархий (МАИ)

Для объективного определения весов w_j был применен метод анализа иерархий Т. Саати [5]. Экспертам (ИТ-руководству вуза) было предложено попарно сравнить критерии по шкале относительной важности от 1 до 9. На основе заполненной матрицы попарных сравнений (табл. 1) был вычислен вектор приоритетов (весов).

Таблица 1. Матрица попарных сравнений критериев доступности

Критерий	**A_1**	**A_2**	**A_3**	**A_4**
A_1	1	1/2	2	3

Критерий	**A_1**	**A_2**	**A_3**	**A_4**
A_2	2	1	3	4
A_3	1/2	1/3	1	2
A_4	1/3	1/4	1/2	1

Процедура расчета включала следующие шаги:

1) вычисление суммы элементов каждого столбца;

2) деление каждого элемента матрицы на сумму столбца (нормализация);

3) расчет среднего арифметического каждой строки нормализованной матрицы, что и дает искомый вектор весов.

В результате получены следующие весовые коэффициенты: $w_1 \approx 0.28$, $w_2 \approx 0.47$, $w_3 \approx 0.16$, $w_4 \approx 0.09$. Коэффициент согласованности (ОС) составил 0.05 (< 0.1), что свидетельствует о непротиворечивости экспертных оценок.

2. Результаты.

2.1. Расчет коэффициента А для моделируемого сценария

Для демонстрации работы методики проведено моделирование для базового сценария работы СЗИ в вузе. Исходные данные и результаты расчета представлены в табл. 2.

Таблица 2. Исходные данные и расчет коэффициента А для базового сценария

Показатель	**Обозначение**	**Значение**	**Расчет частного показателя**	**A_j**
Общее время, ч	$t_{общ}$	720 (30 дн.)	-	-
Время простоя сервисов, ч	$t_{простоя}$	12	$A_1 = \frac{720 - 12}{720}$	0.983
MTTF сети, ч	$MTTF_{сети}$	718	$A_2 = 1 - \frac{2}{718 + 2}$	0.997
MTTR сети, ч	$MTTR_{сети}$	2		
Всего обращений	$C_{общее}$	3 000 000	$A_3 = 1 - \frac{1500}{3000000}$	0.9995
Ложные блокировки	$C_{ложных}$	1500		
Всего пользователей	$U_{общее}$	7500	$A_3 = 1 - \frac{38}{7500}$	0.995
Пользователи с жалобами	$U_{жалоб}$	38		

Интегральный коэффициент доступности рассчитывается по формуле (1):

$A = 0.28 \times 0.983 + 0.47 \times 0.997 + 0.16 \times 0.9995 + 0.09 \times 0.995 \approx 0.993$.

Полученное значение $A = 0.993$ свидетельствует о высоком уровне доступности образовательной среды.

2.2. Интерпретация результатов и шкала оценки

Для практического использования методики предложена трехуровневая шкала оценки коэффициента A, адаптированная к требованиям непрерывности учебного процесса:

- **Отличная доступность:** $A \geq 0.990$. Простои практически не влияют на учебный процесс.
- **Удовлетворительная доступность:** $0.970 \leq A < 0.990$. Наблюдаются кратковременные сбои, требующие мониторинга и планового улучшения.
- **Неприемлемая доступность:** $A < 0.970$. Систематические нарушения, требующие немедленного вмешательства.

2.3. Комплексная эффективность СЗИ

Предлагаемый коэффициент A является не только инструментом диагностики, но и ключевым элементом для комплексной оценки эффективности всей СЗИ. Традиционно эффективность средства защиты (Q_{S0}) оценивается по его способности нейтрализовать угрозы с учетом его готовности. В рамках теории массового обслуживания и надежности это может быть выражено как:

$$Q_{S0} = k_r \times P_S \qquad (7)$$

где k_r — коэффициент готовности средства защиты (доля времени его работоспособности), P_S — вероятность успешного обнаружения и нейтрализации угрозы при его работе.

Однако показатель Q_{S0} отражает лишь тактическую эффективность в идеализированных условиях. В реальной эксплуатации средство защиты взаимодействует с пользователями и инфраструктурой, влияя на доступность.

Для учета этого влияния вводится показатель комплексной (стратегической) эффективности СЗИ (Q_{S1}):

$$Q_{S1} = Q_{S0} \times A \qquad (8)$$

Данная формула отражает фундаментальный компромисс: система защиты не может считаться полностью эффективной, если, обеспечивая безопасность, она парализует основную деятельность организации. Показатель (Q_{S1}) стремится к максимуму, когда одновременно достигаются высокие значения как технической защищенности (Q_{S0}), так и доступности среды (A).

Подход к интегральной оценке, объединяющей показатели безопасности и операционной эффективности, находит свое развитие в современных исследованиях по моделированию ИТ-систем [6].

Пример расчета комплексной эффективности:

Рассмотрим сценарий для моделируемого вуза. Допустим, в качестве ключевого средства защиты используется межсетевой экран (МЭ) со следующими характеристиками:

Коэффициент готовности МЭ (простой 2 часа в месяц): $k_r = 0.997$

Вероятность нейтрализации атаки: $P_S = 0.98$.

Значение коэффициента доступности среды (из табл. 2): $A = 0.993$.

Тогда:

Тактическая эффективность МЭ: $Q_{S0} = 0.997 \times 0.98 \approx 0.977$.

Комплексная эффективность СЗИ: $Q_{S1} = 0.977 \times 0.993 \approx 0.970$.

Таблица 3. Шкала оценки для Комплексной эффективности

Соотношение	**Уровень эффективности**	**Интерпретация**
$Q_{S1} \geq 0.95 \times (Q_{S0} \times 0.99)$	Оптимальный	Система защиты обеспечивает высокую техническую эффективность (Q_{S0}) и минимальное воздействие на доступность

		(A→1). Находится в зоне наилучшего компромисса.
$0.80 \times (Q_{S0} \times 0.99) \leq Q_{S1} < 0.95 \times (Q_{S0} \times 0.99)$	Приемлемый	Наблюдается дисбаланс: либо безопасность слегка жертвуется ради доступности, либо наоборот. Требует тонкой настройки.
$Q_{S1} < 0.80 \times (Q_{S0} \times 0.99)$	Дисфункциональный	Конфигурация СЗИ непригодна: либо безопасность не обеспечена, либо доступность учебного процесса неприемлемо низка.

В рассмотренном примере Q_{S1} _эталон = $0.977 \times 0.99 \approx 0.967$. Таким образом, $Q_{S1} = 0.970 > 0.95 \times 0.967 \approx 0.919$, что указывает на нахождение системы в оптимальной зоне. Данный формализованный подход позволяет перейти от качественных споров о приоритете «безопасности» или «доступности» к количественному поиску конфигурации, максимизирующей обобщенный показатель Q_{S1}.

Заключение

В работе разработана методика оценки воздействия системы защиты информации на непрерывность учебного процесса. Ключевым элементом методики является интегральный коэффициент доступности образовательной среды (A), агрегирующий четыре частных показателя с весами, определенными методом анализа иерархий. Апробация методики на моделировании для вуза показала ее практическую применимость для диагностики состояния ИТ-инфраструктуры и обоснования решений по ее развитию. Методика восполняет пробел между техническими оценками защищенности и требованиями к качеству процесса обучения.

Перспективным направлением дальнейших исследований является применение разработанного коэффициента А в качестве критерия для сравнительного анализа и выбора оптимальных архитектурных решений построения СЗИ в образовательных организациях.

Библиографический список

1. Калмуратова С.М. Анализ методов и методика оценки эффективности систем защиты информации // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 450-458.
2. Официальный сайт Роскомнадзора [Электронный ресурс]. – URL: https://rkn.gov.ru/ (дата обращения: 01.04.2024).
3. ГОСТ Р 57580.1-2017. Безопасность финансовых операций. Защита информации. Оценка эффективности средств защиты информации. – М.: Стандартинформ, 2017.
4. Москвитин Г.И., Тараскин М.М., Захаров А.Г. Комплексная защита информации в организации: монография. – СПб.: Лань, 2021. – 295 с.
5. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 278 с.
6. Кузнецов Н.А., Петров С.В. Моделирование комплексной оценки эффективности ИТ-систем с учетом факторов доступности и безопасности // Вестник университета ИТ-безопасность. – 2023. – № 1(12). – С. 34-42.