МЕТОДЫ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Ботиров Сохибжон
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Аннотация. В докладе рассматриваются подходы к оценке информационной безопасности сетей передачи данных (СПД). Проведён анализ методов качественной и количественной оценки рисков, приведены математические модели расчёта риска, схема процесса управления рисками и матрица рисков. Отдельное внимание уделено анализу и управлению рисками в облачных средах с учётом модели разделяемой ответственности.

Abstract. The paper discusses approaches to information security assessment of data communication networks. Qualitative and quantitative risk assessment methods are analysed; mathematical risk models, a risk management process scheme and a risk matrix are presented. Special attention is paid to risk analysis and management in cloud environments under the shared responsibility model.

Ключевые слова: информационная безопасность, сеть передачи данных, анализ рисков, количественная оценка, угроза, уязвимость, облачные технологии, разделяемая ответственность.

Интенсивное развитие информационной инфраструктуры, базирующейся на высокоскоростных сетях передачи данных (СПД), обусловило появление ряда проблем, касающихся информационной безопасности, которые являются одними из наиболее сложных и наукоёмких. Распространение технологий виртуализации, программно-определяемых сетей (SDN) и облачных вычислений существенно расширило периметр защиты и усложнило структуру информационных потоков.

Несмотря на возрастающие усилия по использованию различных мер и средств обеспечения информационной безопасности (ИБ) СПД, их уязвимость не уменьшается, а постоянно возрастает в условиях внедрения новых технологий передачи данных. Поэтому одним из ключевых направлений обеспечения ИБ в СПД является решение вопросов анализа и управления рисками информационной безопасности.

К числу важнейших задач в области обеспечения ИБ СПД относятся:

– разработка требований, критериев, показателей и методов оценки информационной безопасности;

– разработка методов и методик оценки информационной безопасности СПД, в том числе для распределённых и облачных инфраструктур.

В этой связи проблема анализа и управления рисками ИБ СПД является крайне важной и актуальной.

Риск отдельного ресурса в СПД оценивается через ценность его активов, уязвимости, угрозы, реализуемые через эти уязвимости, вероятности их реализации и последствия воздействий. Взаимосвязь этих понятий образует причинно-следственную цепочку формирования риска (рис. 1).

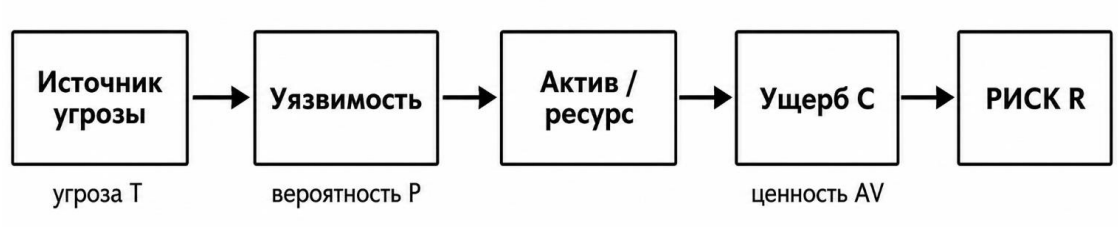

Рисунок 1. Модель формирования риска информационной безопасности

При проведении анализа рисков информационной безопасности в СПД необходимо определить:

– существующие угрозы в СПД и их уровень;
– уязвимые места в СПД;
– состав и эффективность средств обеспечения информационной безопасности СПД;
– комплекс мер, позволяющий снизить риски нарушения информационной безопасности до допустимого уровня.

Сложность выбора комплекса методов и средств обеспечения ИБ СПД обусловлена трудностями учёта многообразия факторов влияния потенциальных угроз и их последствий. Для формирования объективной картины ИБ необходимо организовать систематический сбор и анализ информации о рисках и убытках от их реализации.

Под количественными характеристиками ИБ понимаются числовые значения показателей, позволяющие с достаточной достоверностью оценить текущее состояние защищённости. В базовой модели риск трактуется как произведение вероятности реализации угрозы Р на величину возможного ущерба С:

$$R = P \cdot C \quad (1)$$

Для системы, подверженной множеству независимых угроз, совокупный риск определяется суммированием частных рисков по всем n рассматриваемым угрозам:

$$R = \sum_{i=1}^{n} P_i \cdot C_i \quad (2)$$

Более точная модель учитывает условный характер реализации угрозы через конкретную уязвимость. Если P(Ti) — вероятность возникновения i-й угрозы, P(Vj|Ti) — условная вероятность того, что угроза реализуется через j-ю уязвимость, а Cij — соответствующий ущерб, то интегральный риск равен:

$$R_{\Sigma} = \sum_{i=1}^{n}\sum_{j=1}^{m} P(T_i) \cdot P(V_j \mid T_i) \cdot C_{ij} \quad (3)$$

В стоимостных методах (методология NIST SP 800-30) применяются показатели ожидаемых потерь. Единичные ожидаемые потери SLE рассчитываются как произведение стоимости актива AV на коэффициент воздействия EF (доля утрачиваемой стоимости):

$$SLE = AV \cdot EF \quad (4)$$

Годовые ожидаемые потери ALE получают умножением SLE на среднегодовую частоту возникновения инцидента ARO:

$$ALE = SLE \cdot ARO = AV \cdot EF \cdot ARO \quad (5)$$

Применение средств защиты с эффективностью E ($0 \leq E \leq 1$) снижает исходный риск R0 до остаточного значения:

$$R_{res} = R_0 \cdot (1 - E) \quad (6)$$

Для наглядного качественно-количественного ранжирования рисков применяется матрица рисков, в которой каждая ячейка соответствует произведению уровня вероятности на уровень ущерба (рис. 2). Такой подход позволяет распределить риски по зонам — от низкого до критического — и определить приоритетность мер защиты.

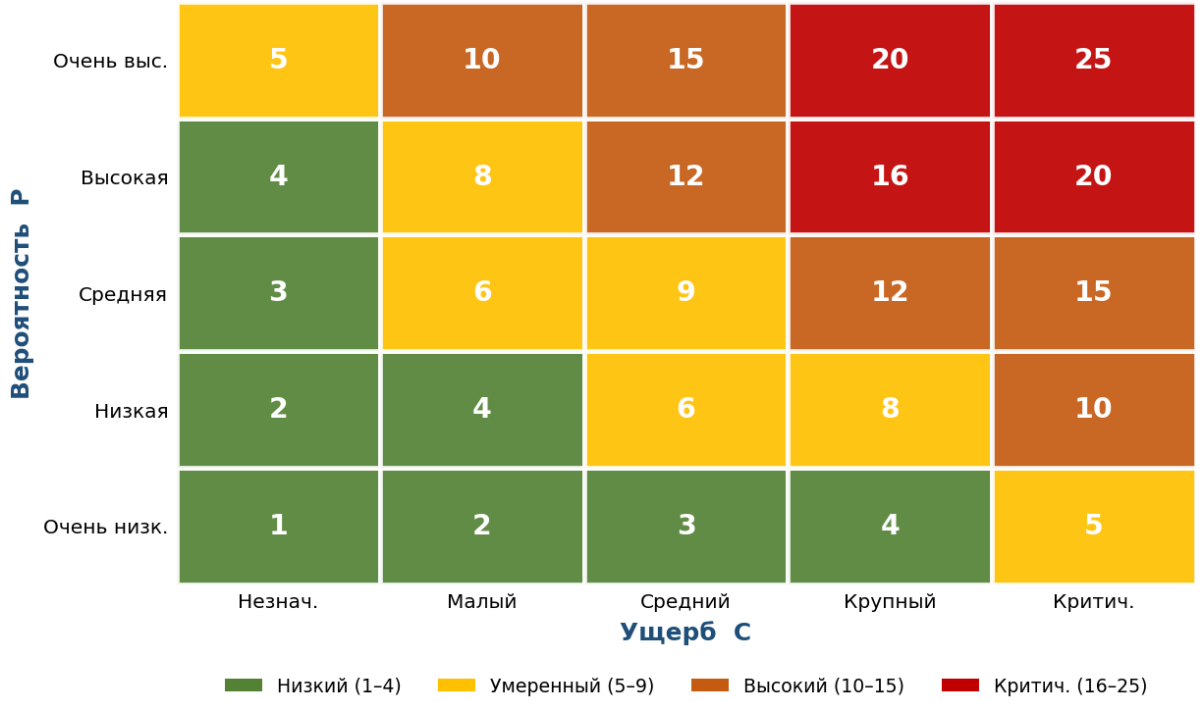

Рисунок 2. Матрица рисков ИБ (R = P × C)

Управление рисками ИБ — это непрерывный циклический процесс, регламентированный стандартами ISO/IEC 27005 и ГОСТ Р ИСО/МЭК 27005. Он включает идентификацию активов и угроз, анализ и количественную оценку рисков, их обработку (снижение, передачу, принятие или избежание) и постоянный мониторинг с пересмотром.

Существующие методы оценки рисков принято делить на качественные, количественные и комбинированные. Их сравнительные характеристики приведены в табл. 1.

Таблица 1

Сравнение методов оценки рисков ИБ

Признак	**Качественные методы**	**Количественные методы**
Форма результата	Шкалы «низкий–средний–высокий»	Числовые значения (деньги, вероятности)
Примеры	OCTAVE, экспертные оценки, матрица рисков	NIST SP 800-30 (ALE), FAIR, CRAMM
Трудоёмкость	Низкая, быстрое применение	Высокая, требует статистики
Объективность	Зависит от экспертов	Воспроизводимая, измеримая

Переход СПД к облачной модели (IaaS, PaaS, SaaS) принципиально меняет характер угроз и распределение ответственности за их обработку: в облаке безопасность обеспечивается совместно — часть мер реализует провайдер, часть клиент. Эта модель разделяемой ответственности (shared responsibility) показана на рис. 4 и служит отправной точкой для корректного анализа рисков.

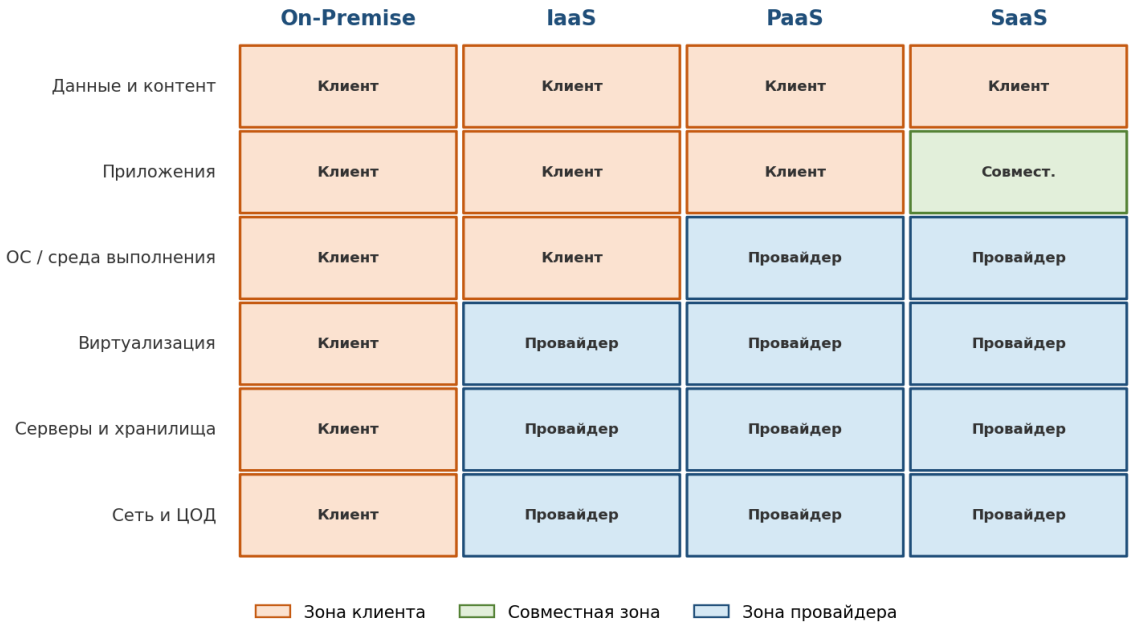

Рисунок 4. Модель разделяемой ответственности за ИБ в облаке

Облачная среда привносит специфические угрозы, отсутствующие или менее выраженные в традиционных СПД:

– риски многоарендности (multi-tenancy) — утечка данных между изолированными виртуальными средами разных клиентов;

– ошибки конфигурации (misconfiguration) облачных сервисов и избыточные права доступа;

– компрометация интерфейсов управления и API провайдера;

– привязка к поставщику (vendor lock-in) и риски доступности при сбоях ЦОД;

– юридические риски, связанные с трансграничной передачей и хранением данных.

С учётом разделяемой ответственности интегральный риск облачной СПД целесообразно рассчитывать как взвешенную сумму частных рисков по зонам, где коэффициент wk отражает долю контроля стороны над k-м элементом инфраструктуры:

$$R_{cloud} = \sum_k w_k \cdot P_k \cdot C_k, \qquad \sum_k w_k = 1 \tag{7}$$

Экономическую обоснованность вложений в защиту оценивают показателем возврата инвестиций в безопасность ROSI, где ALE0 и ALE1 — годовые ожидаемые потери до и после внедрения защиты, а Z — её стоимость:

$$ROSI = \frac{ALE_0 - ALE_1 - Z}{Z} \times 100\% \tag{8}$$

Положительное значение ROSI свидетельствует об экономической целесообразности применяемых мер. Сопоставление типовых угроз облачной СПД с рекомендуемыми мерами их обработки приведено в табл. 2.

Таблица 2

Типовые риски облачной СПД и меры их обработки

Угроза	**Уровень риска**	**Меры обработки**
Утечка данных между арендаторами	Высокий	Шифрование, строгая изоляция, контроль доступа
Ошибки конфигурации	Критический	Автоматизированный аудит (CSPM), политики IaC
Компрометация API/учётных записей	Высокий	MFA, ротация ключей, журналирование
Недоступность сервиса (отказ ЦОД)	Умеренный	Резервирование, мультиоблако, SLA

Рассмотренные количественные модели (формулы 1–6) и матрица рисков позволяют формализовать оценку и ранжирование рисков, а циклический процесс управления обеспечивает их снижение до допустимого уровня. Распространение облачных технологий требует адаптации классических методов с учётом модели разделяемой ответственности, угроз многоарендности и критериев экономической эффективности (ROSI); дальнейшие исследования целесообразно направить на разработку методик автоматизированной оценки рисков для гибридных и мультиоблачных СПД.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Новиков А.А., Устинов Г.Н.; Под ред. Устинова Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. — М.: Радио и связь, 2003.
2. Djurayev R.H., Shomaksudov B.Yu. Analysis of the methods of information integrity provision in data transmission networks. // Proceedings of ICEIC2008. June 24–27, 2008, Tashkent, Uzbekistan, p. 304–306.
3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
4. NIST Special Publication 800-30 Rev. 1. Guide for Conducting Risk Assessments. — NIST, 2012.
5. Cloud Security Alliance. Top Threats to Cloud Computing. — CSA, 2022.