Для цитирования
Лившиц И.И. *Оценка рисков для ИТ-инфраструктуры вуза в задаче обеспечения его устойчивого развития / III Научно-практическая конференция «Стандартизация: траектория науки», приуроченная ко Всемирному дню стандартов, Москва, 15 октября 2025 г. // Информационно-экономические аспекты стандартизации и технического регулирования. 2025. № 6(87). С. 553–557.*

УДК 004.094

ОЦЕНКА РИСКОВ ИТ-ИНФРАСТРУКТУРЫ ВУЗА В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ ЕГО УСТОЙЧИВОГО РАЗВИТИЯ

Лившиц И.И., *д-р техн. наук, ФГБУ Университет ИТМО, Россия, г. Санкт-Петербург*

Проблема оценки рисков для ИТ-инфраструктуры для высших учебных заведений (вуз) продолжает оставаться актуальной, несмотря на существующие системы требований, разработанные регуляторами в Российской Федерации. В представленной публикации изучается проблема оценивания рисков применительно к ИТ-инфраструктуре вузов, в том числе и риски поставщиков сервисов, которые недостаточно изучены экспертами в области информационной безопасности (ИБ). Акцент представленной работы сделан на обеспечении устойчивого развития вузов в России, что может быть обеспечено только при соответствующем уровне безопасности ИТ-инфраструктуры и управления полным циклом рисков ИБ.

Ключевые слова: устойчивое развитие, вуз, угрозы, риски, утечки, уязвимости, оценка рисков, остаточный риск, атаки по сторонним каналам, сервисы.

RISK ASSESSMENT FOR THE UNIVERSITY'S IT INFRASTRUCTURE IN ASPECTS TO ENSURE THE SUSTAINABLE DEVELOPMENT

Livshitz I.I., *Doctor of Technical Sciences, ITMO University, St.Petersburg*

The problem of risk assessment for IT-infrastructure for Higher education institutions continues to be relevant even despite the availability of regulatory documentation developed by various regulators. The presented paper examines the problem of risk assessment for the IT-infrastructure for Universities, including the risks of service providers that have not been sufficiently studied by experts in the field of information security. The emphasis of the presented work is on ensuring the sustainable development of Universities in Russia, which can be ensured only with an appropriate level of IT-infrastructure security and management of the full cycle of IT-security risks.

Keywords: open Sustainable development, University, threats, risks, leaks, vulnerabilities, risk assessment, residual risk, attacks third-party channels, services.

Введение

Проблематика оценивания рисков в целом для ИТ-инфраструктуры учреждений высшей школы и конкретно вузов следует признать важной и актуальной. Прежде всего, следует принять во внимание, что ИТ-системы вузов собирают и обрабатывают значительные массивы информации (о сотрудниках, обучающихся, их представителях и пр.). В целях соответствия требованиям регуляторов (например, ФСТЭК России) в ИТ-инфраструктуре многих вузов применяются рекомендованные средства защиты информации (СЗИ). Из практики известно, что факт наличия некоторых СЗИ не является сам по себе универсальной гарантией от злонамеренных воздействий на ИТ-инфраструктуру вуза, хотя бы по причине возможности атак Zero-day («нулевого дня»).

В предложенной публикации представлен подход, который предлагает планировать обеспечение устойчивого развития вуза с учетом проявления рисков для ИТ-инфраструктуры в равной мере изнутри (от работников вуза), так и вне периметра, например, от поставщиков внешних сервисов. Соответственно, любая организация, и вуз в том числе, не имеет

возможности в силу известных граничных условий (бюджет, время, персонал) блокировать абсолютно все существующие технические каналы утечки информации. С учетом данного обстоятельства предлагается новое решение, учитывающее системное безопасное взаимодействие вуза с различными поставщиками (работодателями, рейтинговыми агентствами, поставщиками образовательного контента и пр.), что обеспечивает требуемый уровень безопасности собственной ИТ-инфраструктуры.

Атаки на вузы через сторонние каналы

Из практики хорошо известно, что инциденты на объектах критической информационной инфраструктуры (КИИ) могут приводить к значительным прерываниям нормальной деятельности, а вузы относятся к объектам КИИ в соответствии с требованиями ФЗ-187 [1–2]. С определенной долей уверенности можно полагать, что реализация инцидентов на объектах КИИ является следствием ограниченных бюджетов, которые многие вузы имеют возможность выделять на развитие ИТ-инфраструктуры, и в частности на внедрение достаточного количества СЗИ.

В свою очередь, закупка и внедрение СЗИ в каждом конкретном вузе представляются нетривиальной задачей, поскольку нужно доказать руководству, какие именно риски компрометации ИТ-инфраструктуры могут произойти, с каким ущербом (в случае реализации инцидента) и с какой вероятностью. Такое аналитическое обоснование сделать непросто, хотя известны некоторые обзоры, например «2024 Data Breach Investigations Report»[1]. Существующих СЗИ может быть недостаточно, даже если они обеспечивают сложные механизмы аутентификации[2] при защите от риска компрометации со стороны третьих лиц (примеры приведены в обзоре Forbes[3]). Для корректного анализа, оценки и обработки рисков для ИТ-инфраструктуры вузов нужно точно определить возможные каналы реализации инцидентов. Таким образом, проблема реализации полного цикла управления рисками ИТ-инфраструктуры для вузов является актуальной с учетом накопления и обработки значительного объема чувствительных данных, в том числе персональных данных (студентов, преподавателей, приглашенных экспертов и пр.), а также ценных коммерческих, научных и практических результатов деятельности, в том числе с международным участием.

Оценка рисков ИТ-инфраструктуры для вузов

Рассмотрим возможное решение поставленной выше проблемы формирования полного цикла управления рисками ИТ-инфраструктуры для вузов, основываясь на риск-ориентированной системе международных стандартов: ISO/IEC серии 27005[4] и ISO/IEC серии 31000[5]. В данной работе предлагается обеспечить качественную оценку рисков ИТ-инфраструктуры на основании методики управления рисками, включающей выбор из доступной базы данных угроз ФСТЭК (БДУ ФСТЭК) угроз безопасности информации (УБИ), определения критериев для принятия рисков (остаточных рисков) и выбор необходимых СЗИ [3–5]. В табл. 1 рассмотрен пример качественной оценки рисков ИТ-инфраструктуры для обобщенного вуза.

Таблица 1

Результаты качественной оценки рисков ИТ-инфраструктуры для вузов

Тип угроз	Угрозы	Активы	Риск			Критерий риска	Решение	Остаточный риск			Решение
			Вер.	Посл.	Знач.			Вер.	Посл.	Знач.	
Физические	Воздействие огня, воды	Здания Линии связи Электро-снабжение	Средняя	Высокие	Средний	Средний	Передать	Низкая	Средние	Низкий	Принять

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.securitylab.ru/news/547531.php
[3] https://www.forbes.com/sites/sungardas/2014/09/04/youve-completed-a-vendor-risk-assessment-now-what/
[4] https://docs.cntd.ru/document/1200084141
[5] https://docs.cntd.ru/document/1200170125

Тип угроз	Угрозы	Активы	Риск			Критерий риска	Решение	Остаточный риск			Решение
			Вер.	Посл.	Знач.			Вер.	Посл.	Знач.	
Окружающая среда	Стихийные бедствия	Здания Линии связи Электро-снабжение	Средняя	Высокие	Средний	Средний	Передать	Низкая	Средние	Низкий	Принять
Инфраструктура	Блокирование кабельных линий	Здания Линии связи Электро-снабжение	Средняя	Средние	Средний	Средний	Передать	Низкая	Средние	Низкий	Принять
Человеческий фактор	Удаление / кража данных	Любые компоненты	Низкая	Средние	Низкий	Средний	Принять				
Поставщик сервисов	Блокирование кабельных линий	Здания Линии связи Электро-снабжение	Низкая	Средние	Низкий	Средний	Принять				

Обозначение:

1. Вер. – вероятность (градации: высокая (В), средняя (Ср), низкая (Н));
2. Посл. – последствия (градации: высокие (В), средние (Ср), низкие (Н));
3. Знач. – значение риска (градации: высокий (В), средний (Ср), низкий (Н)).

Пример качественной оценки рисков ИТ-инфраструктуры для вузов отражает различные типы УБИ, в том числе внешние по отношению к вузу – УБИ по сторонним техническим каналам, которые вуз не в состоянии контролировать. Таким образом, объективно, для обеспечения необходимой непрерывности всей ИТ-инфраструктуры вуза, может быть выбран такой вариант обработки риска, как «передача». В этом случае вуз выбирает по системе объективных показателей надежного поставщика сервисов, который минимально имеет необходимый опыт, лицензии и квалифицированный персонал. Определенно в реальном примере ИТ-инфраструктуры для конкретного вуза могут применяться и другие методы обработки рисков в отношении внешних каналов, а также их комбинации. В частности, может применяться дополнительное страхование финансовой ответственности в случае стихийных бедствий (как метод «разделения» ответственности).

Расчет рисков ИТ-инфраструктуры для вуза

На основании указанных выше международных стандартов ISO/IEC серии 27005 и ISO/IEC серии 31000 определим формулу для расчета рисков ИТ-инфраструктуры для вуза. С учетом важного акцента на обеспечении безопасности ИТ-инфраструктуры вуза предлагается следующая формула (1):

$$R_{\text{ВУЗ}} = \sum_{j}^{m} S_j \, L_j k_j \qquad (1)$$

где:

S_j – показатель последствий;

L_j– показатель вероятности;

K_j – коэффициент значимости.

В формуле (1) коэффициент k_j необходим для объективного оценивания значимости конкретного риска Rj с учетом выбранного ранее множества УБИ (m). Соответственно, необходимо ввести новое ограничение R_{Cr}, поскольку полный цикл идентификации, оценки, анализа и обработки всех возможных рисков для современной ИТ-инфраструктуры вуза не представляется экономически возможным. Таким образом, с учетом нового ограничения R_{Cr}, формула риска принимает вид (2):

$$R_{\text{вуз}} = \sum_{j}^{m} S_j \, L_j k_j \mid R_j \geq R_{Cr} \qquad (2)$$

Таким образом, удобно сопоставить две формулы, начальную (1) и дополненную (2), для оценки рисков применительно для ИТ-инфраструктуры вуза. В качестве примера установим

простые граничные условия: z – количество технических каналов передачи критичных данных в ИТ-инфраструктуре вузов:

- для «внутренней» модели, без учета поставщиков сервисов ($z \leq 5$);
- для «внешней» модели, с учетом коммуникаций с поставщиками сервисов ($z \geq 10$).

Результаты качественной оценки рисков ИТ-инфраструктуры для вузов по дополненной формуле (2) представлены в табл. 2.

Таблица 2

Результаты качественной оценки рисков ИТ-инфраструктуры для вузов по дополненной формуле (2)

Тип модели	Потенциальный нарушитель	Риски	Оценка риска			Кр. риска	Решение	Дополнительные меры		Остаточный риск			Финальное решение
			Вер.	Посл.	Знач.			Техн.	Организ.	Вер.	Посл.	Знач.	
«Внутренняя модель» (формула 1)	Учащиеся	Человеческий фактор	Н	Ср	Н	Ср	Принять						
	Работники	Человеческий фактор	Ср	Ср	Ср	Ср	Обработка	DLP	Контракт	Н	Ср	Н	Принять
	ФОИВ	Доступность	Н	Н	Н	Ср	Принять						
«Внешняя модель» (формула 2)	Учащиеся	Человеческий фактор	Н	Ср	Н	Ср	Принять						
	Работники	Человеческий фактор	Ср	Ср	Ср	Ср	Обработка	DLP	Контракт	Н	Ср	Н	Принять
	ФОИВ	Доступность	Н	Ср	Н	Ср	Принять						
	Провайдеры	Доступность	Н	В	Ср	Ср	Обработка	Резерв	Контракт	Н	Ср	Н	Принять
	Поставщик СЗИ	Человеческий фактор	Н	Ср	Н	Ср	Принять						
	Поставщик контента	Человеческий фактор	Н	Н	Н	Ср	Принять						
	СМИ	Человеческий фактор	Ср	Ср	Ср	Ср	Обработка	DLP	Контракт	Н	Ср	Н	Принять
	Рейтинговые агентства	Человеческий фактор	Ср	Н	Н	Ср	Принять						
	Работодатели	Человеческий фактор	Ср	Н	Н	Ср	Принять						
	Рекрутеры	Человеческий фактор	Ср	Н	Н	Ср	Принять						

Примечания:

1. Вер. – вероятность (градации: высокая (В), средняя (Ср), низкая (Н));
2. Посл. – последствия (градации: высокие (В), средние (Ср), низкие (Н));
3. Знач. – значение риска (градации: высокий (В), средний (Ср), низкий (Н)).

Заключение

Предложенная публикация кратко характеризует новый метод качественной оценки рисков применительно к ИТ-инфраструктуре для вузов в Российской Федерации. Новый метод объективно предполагает учет и обработку значительно большего количества внешних по отношению к вузу угроз безопасности, и прежде всего – реализуемых по сторонним техническими каналам. Такое расширение ландшафта современных угроз обеспечивает более четкое и обоснованное формирование и обоснование необходимых ресурсов (финансы, оборудование, персонал) для снижения рисков ИТ-инфраструктуры для вузов. Полученные результаты расчетов могут рассматриваться при обеспечении безопасности вузов в Российской Федерации.

Список литературы

1. Лившиц И.И., Лившиц М.И. Применение национальных стандартов ГОСТ Р и международных стандартов ISO серии 31000 для обеспечения современного уровня менеджмента рисков // Управление финансовыми рисками. 2022. № 4. С. 312–323.
2. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 1. Аналитический обзор. // Газовая промышленность. – 2022. – № 9. – С. 40–56.

3. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 2. Новая разработка. // Газовая промышленность. – 2022. – № 11. – С. 50–70.
4. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа. Вопросы кибербезопасности. – 2020. – № 1 (35). – С. 42 – 51.
5. Орешкина А.С., Лившиц И.И., Соколов Е.О. Правовые проблемы деятельности инспекторов по защите персональных данных: содержание, особенности, специфика для нефтегазовых компаний холдингового типа // Газовая промышленность. 2023. № 4 (847). С. 96–104.

References

1. Livshits I.I., Livshits M.I. Application of national GOST R standards and international ISO 31000 series standards to ensure a modern level of risk management // Financial risk management. 2022. No. 4. Pp. 312–323.
2. Livshits I.I., Sokolov E.O., Lukyanova A.A. Circuit solutions for the practical implementation of secure electronic document management. Part 1. Analytical review. // Gas industry. – 2022. – No. 9. – Pp. 40–56
3. Livshits I.I., Sokolov E.O., Lukyanova A.A. Circuit solutions for the practical implementation of secure electronic document management. Part 2. New development. // Gas industry. – 2022. – No. 11. – Pp. 50–70.
4. Livshits I.I. The practice of cyber risk management in oil and gas projects of holding companies. Cybersecurity issues. – 2020. – №1 (35). – Pp. 42–51.
5. Oreshkina A.S., Livshits I.I., Sokolov E.O. Legal problems of personal data protection inspectors: content, features, specifics for oil and gas companies of the holding type // Gas Industry. 2023. No. 4 (847). Pp. 96–104.