ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.094

DOI: 10.21822/2073-6185-2025-52-1-97-104 Оригинальная статья /Original article

Оценка рисков утечки персональных данных от атак по каналам поставщиков

И.И. Лившиц
Национальный исследовательский университет ИТМО,
197101, г. Санкт-Петербург, Кронверкский проспект, д. 49, Россия

Резюме. Цель. Проблема защиты персональных данных (ПДн) продолжает оставаться актуальной даже несмотря на более чем значительное количество нормативной документации, разработанной различными регуляторами. Целью исследования является разработка методов оценки риска утечки персональных данных от атак злоумышленников по каналам поставщиков. **Метод.** В представленной работе исследуется проблема защиты ПДн в информационных системах ВУЗов через сторонние каналы – поставщиков сервисов (supply chain attack), которые, в большинстве случаев, недостаточно изучены экспертами в области информационной безопасности. **Результат**. В отличие от известных «коммерческих» предложений, предусматривающих внедрение новых мер защиты (ограниченных только бюджетом), предлагается применять метод оценки рисков утечки ПДн по всем существующим каналам циркуляции ПДн, а не только для простейшего формализованного выполнения требований владельца ПДн. Акцент представленной работы сделан на обеспечении защиты ПДн для ВУЗов в РФ. Изучены несколько каналов распространения ПДн по основным критическим направлениям (предоставления учебного контента, данных абитуриентов и их представителей, запросов работодателей и пр.). **Вывод.** Представленные результаты могут быть востребованы как в учебном процессе для программ обучения по специальности «Информационная безопасность», так и экспертами, занимающимися практическими аспектами обеспечения защиты ПДн в ВУЗах.

Ключевые слова: персональные данные, ВУЗ, угрозы, риски, утечки, уязвимости, оценка рисков, остаточный риск, атаки по сторонним каналам, сервисы

Для цитирования: И.И. Лившиц. Оценка рисков утечки персональных данных от атак по каналам поставщиков. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(1):97-104. DOI:10.21822/2073-6185-2025-52-1-97-104

Assessment of the risks of personal data leakage from through supplier channel attacks

I.I. Livshits
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. Objective. The problem of personal data (PD) protection continues to be relevant even despite the more than significant amount of regulatory documentation developed by various regulators. The aim of the study is to develop methods for assessing the risk of personal data leakage from malicious attacks through supplier channels. **Method.** The presented paper examines the problem of protecting personal data in information systems of universities through third–party channels – service providers (supply chain attack), which, in most cases, have not been sufficiently studied by experts in the field of IT-security. **Result.** Unlike the well-known "commercial" proposals providing for the introduction of new and new countermeasures (limited only by the budget), it is proposed to apply the method of assessing the risks of PD leakage through all existing PD circulation channels, and not only for the simplest formalized fulfillment of the requirements of the PD owner. The focus of the presented work is on ensuring the protection of PD for Universities in the Russian Federation, accordingly, several channels for the dis-

semination of PD in the main critical areas (provision of educational content, data of applicants and their representatives, requests from employers, etc.) were studied. **Conclusion.** The presented results can be in demand both in the educational process for University programs in the specialty "Information Security", and by experts dealing with practical aspects of ensuring the protection of PD in Universities.

Keywords: personal data, University, threats, risks, leakage, vulnerability, risk assessment, residual risk, attacks through third-party channels, personal data, service

For citation: I.I. Livshits. Assessment of the risks of personal data leakage from through supplier channel attacks. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(1):97-104. (In Russ) DOI:10.21822/2073-6185-2025-52-1-97-104

Введение. Проблема защиты ПДн для ВУЗов не является уникальной, но именно в настоящее время многие эксперты обратили внимание на необходимость обеспечения надлежащей защиты этой ценной категории информации от злоумышленников, готовых похитить и «монетизировать» любые данные. Определенно, ВУЗы, как и многие государственные организации (примем обобщение, поскольку в РФ успешно работает значительное количество и частных и отраслевых ВУЗов), применяют различные средства защиты информации (СЗИ), прошедшие в установленном порядке сертификацию регуляторов (например ФСТЭК или ФСБ). Однако следует признать, что сам факт применения СЗИ не является абсолютной гарантией защиты от утечки ПДн, поскольку существуют уязвимости (в том числе «нулевого дня») технических и программных компонент информационных систем (ИС), внутренние и внешние злоумышленники и пр.

Постановка задачи. В представленной публикации рассмотрен новый подход, учитывающий, что утечки ПДн могут быть не только из «периметра» ВУЗа, но также от третьих лиц, например, поставщиков сервисов для ВУЗов (например, образовательного контента). Необходимо принять во внимание, что собственные ИС поставщиков сервисов могут содержать критические уязвимости. В общем случае, ВУЗ не сможет в силу известных ограничений контролировать надежно все возможные каналы утечки информации, соответственно, невозможно «закрыть» потенциальные уязвимости во многих ИС поставщиков сервисов. Предложено новое архитектурное решение, которое учитывает системное взаимодействие ИТ-инфраструктуры ВУЗов с различными ИС, принадлежащими как государственными органам (министерствам и ведомствам), так и частным компаниям (работодателям, рейтинговым агентствам, поставщикам образовательного контента и пр.)

Методы исследования. Атаки через сторонние каналы (атаки через поставщиков). В настоящее время известно о многих критических инцидентах, связанных с утечкой ПДн крупнейших компаний во всем мире. Проблема утечки ПДн является актуальной практически для всех отраслей, и в настоящее время не предполагается уникальной успешной реализации экономически обоснованной и в тоже время достаточной единой системы мер защиты [21–24]. К сожалению, в равной мере эта проблема затрагивает и бюджетные организации, которые напрямую не имеют дорогостоящих коммерческих данных, но в тоже время не обладают такими же значительными бюджетами на обеспечение ИБ, как промышленные, финансовые или оборонные компании. Следует признать, что интерес к различным категориями ПДн имеет вполне существенный ресурс «монетизации», поскольку стоимость взлома ИТ-инфраструктуры ВУЗа существенно ниже, чем, например, у оборонных предприятий, что позволяет получать доход. Не обязательно атаковать крупные компании, известен пример утечки более 2 млн. личных данных клиентов от простого поставщика офтальмологического ПО [1].

В отчете «2024 Data Breach Investigations Report», представленный компанией Verizon [2], показано (рис. 1), что доля инцидентов и случаев компрометации в отрасли образование (Education) существенно велика и превышает такие отрасли как финансы (Finance) и производство (Manufacturing). Конкретно проблема утечки ПДн актуальна

для ВУЗов во всем мире, например: в Университете Хайфы [3], Манчестера [4]или Швейцарии [5]. Как показывает статистика, существующих мер защиты ПДн (даже таких многоступенчатых, как многофакторная аутентификация [6]) явно недостаточно.

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

Рис. 1 – Количество инцидентов и случаев компрометации по отраслям 2024 г.
Fig. 1 – Number of incidents and cases of compromise by industry in 2024.

В экспертном сообществе справедливо полагают важным обратить внимание на риски утечки ПДн через сторонние каналы при атаках «третьих лиц» [7]. В отчетах Forbes [8] отмечается: «… К счастью, существует масса вариантов избежать данного риска, равно как и многих других, которые могут быть обнаружены в процессе оценки рисков третьих сторон». В указанном выше отчете компании Verizon представлен подробный анализ типов угроз, которые были реализованы в рассмотренных случаях компрометации, показано, что почти 15% всех утечек произошли с участием третьих сторон (рис. 2). Существенно и то, что в эту категорию включены и случаи компрометации из-за уязвимостей в ПО, что, к сожалению, в полной мере затрагивает и ИТ-инфраструктуру ВУЗов, не имеющих достаточных ресурсов для создания собственных безопасных программных компонентов.

Рис. 2 – Статистика случаев компрометации по типам угроз 2024 г.
Fig. 2 – Statistics of compromise cases by threat type in 2024.

Дополнительно можно отметить еще несколько специфических атак по сторонним каналам, в т.ч. по каналам поставщиков сервисов [9]. В качестве российской аналитической базы следует рассмотреть актуальный отчет (май 2024) «Утечки информации в избранных отраслях, 2021-2023 годы», который представлен Экспертно-Аналитическим центром InfoWatch [10]. Отметим, что в РФ в области защиты ПДн применяется следующая нормативная база, кратко: Федеральные законы (N 152-ФЗ, N 149-ФЗ, N 63-ФЗ и др.),

постановления Правительства (например: N 1119), приказы ФСТЭК (например: N 21, N 235, N 77), приказы ФСБ (например, N 378). Для защиты ПДн персональных многие организации применяют известный европейский стандарт GDPR [25]. Соответственно, с учетом краткого анализа отметим, насколько важно защищать ВУЗы, поскольку они реально оперируют сотнями тысяч записей личных данных самых различных категорий субъектов ПДн (студентов, их законных представителей, работников, рецензентов, научных руководителей, приглашенных экспертов и пр.). При более детальном анализе ситуация выглядит еще более угрожающей, поскольку во многих ВУЗах реализуются программы обучения и академической мобильности для иностранных граждан (студентов, аспирантов и преподавателей).

Обсуждение результатов. В представленной работе предлагается решение поставленной выше проблемы, основываясь на современной риск-ориентированной нормативной базе – ГОСТ Р ИСО/МЭК (ISO/IEC) серии 27005 [11]и ГОСТ Р ИСО/МЭК (ISO/IEC) 31000 [12]. Предлагается формирование численной оценки рисков утечки ПДн в соответствии с известной методикой управления рисками, включающей определение угроз безопасности информации (УБИ), например, на базе доступной базы данных угроз ФСТЭК (БДУ ФСТЭК), установления критерия для принятия рисков, оценка рисков (по показателям вероятности и последствий), выбор мер защиты, оценки результативности мер защиты и оценки остаточных рисков на финальном этапе [26-29].

В табл. 1 представлен фрагмент качественной оценки рисков утечки ПДн, выполненный в 2024 г. в Университете ИТМО в рамках практических работ по курсу «Нормативно-методическое обеспечение информационной безопасности».

Таблица 1. Результаты качественной оценки рисков утечки ПДн для ВУЗа
Table 1. Results of the qualitative assessment of the risks of personal data leakage for the university

Тип угроз	Примеры угроз	Подвержены активы	Риск			Критерий риска	Решение	Остаточный риск			Решение
			В	П	Р			В	П	ОР	
Физические	Воздействие огня, воды	Здания ЦОД Линии связи	Крайне низкая	Критические	Низкий	Средний	Принять	-	-	-	
Окружающая среда	Стихийные бедствия	Здания ЦОД Линии связи	Крайне низкая	Критические	Низкий	Средний	Принять	-	-	-	
Инфраструктура	Нарушение кабельных линий	Здания ЦОД Линии связи	Средняя	Средние	Средний	Средний	Передать (ЦОД)	Низкая	Средние	Низкий	Принять
Технические сбои	Отказ оборудования	Здания ЦОД Линии связи	Низкая	Средние	Низкий	Средний	Принять	-	-	-	
Человеческий фактор	Удаление / кража данных	Все возможные активы	Средняя	Средние	Средний	Средний	Обработка	Низкая	Средние	Низкий	Принять
Провайдер	Удаление данных	Здания ЦОД Линии связи	Средняя	Средние	Средний	Средний	Передать (ЦОД)	Низкая	Средние	Низкий	Принять

Обозначение: В – вероятность. П – последствия. Р – риск. ОР – остаточный риск. ЦОД – центр обработки данных

Представленный выше пример анализа рисков ПДн включает также и пример обработки рисков с целью формирования оценки «качества» обработки и принятия остаточных рисков. Как показано в примере, в ИТ-инфраструктуре ВУЗа учтены не только «собственные» типы УБИ, но и УБИ по сторонним каналам, например от провайдеров. Этот пример позволяет принять во внимание, что для современного ВУЗа (например, во время приемной компании) обеспечение доступности Web-сайта является исключительно приоритетной задачей. Даже сложно представить совокупность прямых и непрямых (имиджевых) потерь для крупнейших ВУЗов, если в самый разгар приемной кампании сайт будет недоступен несколько часов (дней). На примере простоя сервисов СДЭК известны примерные оценки прямых затрат (по данным РБК [13] – около миллиарда руб. в неделю или около 140 млн. руб. в день), не считая возможных исков и репутационных потерь. Соответственно, логичным и абсолютно обоснованным представляется выбор метода обработ-

ки такого риска как «передача», например, надёжному поставщику услуг, имеющему несколько территориально распределенных ЦОД (имеющих необходимые лицензии и сертификаты) и соответствующую репутацию.

Предлагается новая методика, которая учитывает «циркуляцию» ПДн не только в «традиционном» привычном контуре ИТ-инфраструктуры и известных «внутренних» ИС для ВУЗа, но также и для различных схем внешнего взаимодействия, например (рис. 3): поставщики контента; СМИ; работодатели; рейтинговые агентства; рекрутинговые агентства; министерства и ведомства; поставщики сервисов; поставщики средств защиты (он не могут давать абсолютную гарантию надежности своих решений).

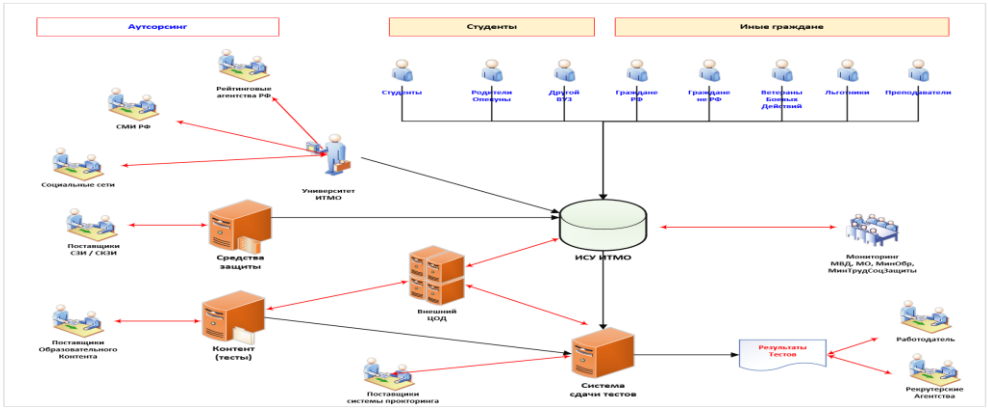

Рис. 3 – Пример ИТ-инфраструктуры Университета ИТМО
Fig. 3 – Example of IT infrastructure of ITMO University

В частности, рассмотрим актуальную информацию компании СКБ «Контур» [14] по возможности организации «бесшовного» взаимодействия между государственными ведомствами и бизнесом. Предполагается, что интеграция ведомственного ЭДО и сервисов для коммерческих систем ЭДО позволит обеспечить безопасный и эффективный обмен документами, поскольку, по информации главы Минцифры России Максута Шадаева, в настоящий момент 20% входящих документов в министерство бизнес подает на бумаге. Важно обратить внимание, что предложенная новая методика учитывает и необходимость защиты функций аутсорсинга (что в настоящее время не учитывается в действующей нормативной базе).

В соответствии с известными стандартами (например, ГОСТ Р ИСО серии 31000 [15] или 27005 [16]), риск определяется как комбинации вероятности и последствий. С учётом требований по защите ПДн в ИТ-инфраструктуре ВУЗа при наличии информационного обмена с ИС третьих сторон, предлагается «базовая» формула оценки риска:

$$R_{ПДн} = \sum_{i}^{n} S_i L_i k_i \qquad (1)$$

где: S_i – последствия; L_i – вероятность; k_i – коэффициент значимости.

В «базовой» формуле (1) коэффициент k_i нужен для приоритезации конкретного риска с учетом актуальных угроз (таблица 1). С учетом рассматриваемой схемы (рис. 3) введем дополнительное критериальное ограничение R_{Cr}, поскольку идентификация, оценка и анализ всех рисков без исключения не представляется целесообразной по причинам ограничения ресурсов (времени, стоимости и доступных экспертов). При условии учета критериальных значений формула риска принимает вид:

$$R_{ПДн} = \sum_{i}^{n} S_i L_i k_i \mid R_i \geq R_{Cr} \qquad (2)$$

Отметим, что значения риска могут определяться различными объективным методами, например по итогам самооценки собственными экспертными группами, по итогам внешнего аудита или по нормативным требованиям (для государственных информационных систем, например, применим приказ ФСТЭК № 17). Рассмотрим далее сопоставление «базовой» (1) и новой «критериальной» (2) формул для оценки рисков ПДн для

ИТ-инфраструктуры ВУЗа с учётом взаимодействия с ИС третьих сторон. Определим следующие граничные условия (n – количество типов каналов циркуляции ПДн): для «внутренней» модели ($n \leq 5$); для «внешней» модели ($n \geq 15$). Новый расчет рисков ПДн представлен в табл. 2.

Таблица 2. Результаты оценки и обработки рисков утечки ПДн для расширенной модели ВУЗа
Table 2. Results of assessment and processing of risks of personal data leakage for the extended model of the university

Тип модели	Ni	Заинтересованные стороны	Риски	Существующие меры	Оценка риска			Критерий риска	Решение	Дополнительные меры		Остаточный риск			Финальное решение
					В	П	Р			Технические	Организационные	В	П	Р	
Без учёта взаимодействия с ИС третьих сторон	1	ВУЗ	Инфраструктура	Контракт	Н	Н	Н	Ср	Принять						
	2	Учащиеся	Человеческий фактор	Соглашение ПДн	Н	Ср	Н	Ср	Принять						
	3	Иные граждане	Человеческий фактор	Соглашение ПДн	Н	Ср	Н	Ср	Принять						
	4	Работники	Человеческий фактор	Соглашение ПДн	Ср	Ср	Ср	Ср	**Обработка**	DLP	Аудиты Соглашения	Н	Ср	Н	Принять
	5	ФОИВ	Доступность	SLA	Н	Н	Н	Ср	Принять						
С учётом взаимодействия с ИС третьих сторон	1.	ВУЗ	Инфраструктура	Контракт	Н	Н	Н	Ср	Принять						
	2.	Учащиеся	Человеческий фактор	Соглашение ПДн	Н	Ср	Н	Ср	Принять						
	3.	Иные граждане	Человеческий фактор	Соглашение ПДн	Н	Ср	Н	Ср	Принять						
	4.	Работники	Человеческий фактор	Соглашение ПДн	Ср	Ср	Ср	Ср	**Обработка**	DLP	Аудиты Соглашения	Н	Ср	Н	Принять
	5.	ФОИВ	Доступность	SLA	Н	Ср	Н	Ср	Принять						
	6.	Провайдеры	Доступность	SLA	Н	В	Ср	Ср	**Обработка**	Резерв	Аудиты Сертификация	Н	Ср	Н	Принять
	7.	Внешний ЦОД	Доступность	SLA	Н	В	Ср	Ср	**Обработка**	Резерв	Аудиты Сертификация	Н	Ср	Н	Принять
	8.	Поставщик СЗИ	Конфиденциальность	SLA	Н	Ср	Н	Ср	Принять						
	9.	Поставщик контента	Конфиденциальность	SLA	Н	Н	Н	Ср	Принять						
	10.	Прокторинг	Конфиденциальность	SLA	Н	Н	Н	Ср	Принять						
	11.	Социальные сети	Конфиденциальность	Соглашение ПДн	Н	Ср	Н	Ср	Принять						
	12.	СМИ	Конфиденциальность	Соглашение ПДн	Ср	Ср	Ср	Ср	**Обработка**	DLP	Аудиты Соглашения	Н	Ср	Н	Принять
	13.	Рейтинговые агентства	Конфиденциальность	Соглашение ПДн	Ср	Н	Н	Ср	Принять						
	14.	Работодатели	Человеческий фактор	Соглашение ПДн	Ср	Н	Н	Ср	Принять						
	15.	Рекрутеры	Человеческий фактор	Соглашение ПДн	Ср	Н	Н	Ср	Принять						

Примечания: 1.Инфраструктура – полная (ИТ, э/э.).2.SLA – Service Level Agreement (соглашение об уровне сервиса);3. ЦОД – центр обработки данных; 4.СЗИ – средство защиты информации; 5.В – вероятность (градации: высокая (В), средняя (Ср), низкая(Н)); 6.П – последствия (градации: высокие (В), средние(Ср), низкие(Н)); 7.Р – значение риска (градации: высокий (В), средний(Ср), низкий(Н)).

Примем во внимание, что установленные граничные условия для новой предложенной модели с учётом взаимодействия с ИС третьих сторон ограничены только информационным взаимодействием, показанным на примере (рис. 3), но известно, что эта модель может быть при необходимости расширена сколь угодно подробно, например, при включении в анализ ИС субподрядчиков. Возможность расширения новой представленной модели можно полагать важным преимуществом. В качестве примеров отметим известные утечки данных специализированных сервисных компаний [17] (в том числе, поставщиков специального ПО [18] и облачных провайдеров [19]).

Предполагается, что включение в новую модель дополнительных вариантов циркуляции ПДн с учётом взаимодействия с ИС третьих сторон позволит более точно описать «ландшафт» УБИ для каждого потенциального источника утечки ПД для конкретного ВУЗа и более эффективно планировать деятельность службы ИБ, в том числе бюджет. Важно, что учитывая итерационный принцип управления рисками ИБ, установленный в указанных выше стандартах, возможно в любой момент пересмотреть как перечень третьих сторон (например, дополнительный ЦОД), так и перечень «наследуемых» рисков с целью более оптимального выбора и применения мер защиты (например, антивирусных систем). Кроме того, ввод нового критериального значения, при котором в новой формуле (2) учитываются только риски, превышающие определенное (пороговое) значение, позво-

ляет перейти к более высокому уровню абстракции – учет риск-аппетита, согласно новейшему ISO/IEC 27005:2022 [20].

Вывод. В представленной работе рассматривается новый метод оценки рисков утечки ПДн по всем существующим каналам циркуляции для ВУЗов в Российской Федерации. В отличие от известных формальных моделей рассматриваются несколько каналов распространения ПДн по основным критическим направлениям (предоставление учебного контента, обработка данных абитуриентов и их представителей, управление запросов работодателей и пр.).

Предложенный новый метод позволяет получить больший охват контроля возможных угроз безопасности информации для информационных систем ВУЗов, в том числе – угроз утечки ПДн по сторонним каналам, что обеспечивает эффективное распределение ресурсов (бюджет, время, персонал). Полученные результаты могут быть применены при реализации проектов защиты ПДН в ВУЗах Российской Федерации, а также в учебном процессе для программ обучения по специальности «Информационная безопасность».

Библиографический список:

1. https://www.securitylab.ru/news/532395.php
2. https://www.verizon.com/business/resources/reports/dbir/
3. https://www.securitylab.ru/news/536418.php
4. https://www.securitylab.ru/news/539183.php
5. https://www.securitylab.ru/news/536310.php
6. https://www.securitylab.ru/news/547531.php
7. https://www.securitylab.ru/blog/personal/achekanov/92297.php
8. https://www.forbes.com/sites/sungardas/2014/09/04/youve-completed-a-vendor-risk-assessment-now-what/
9. https://www.tarlogic.com/blog/supply-chain-attacks/
10. https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-otraslyakh-za-tri-goda
11. https://docs.cntd.ru/document/1200084141?ysclid=lwuuccw1n5461596370
12. https://docs.cntd.ru/document/1200170125?ysclid=lwuube9s8s433673326
13. https://www.rbc.ru/technology_and_media/28/05/2024/6655fc979a79477dbc9e33c4?from=from_main_2
14. https://www.cnews.ru/news/line/2024-06-10_glava_mintsifry_rossii_podderzhal
15. https://internet-law.ru/gosts/gost/73107/?ysclid=ly5sf3zra8363383699
16. ·https://internet-law.ru/gosts/gost/50679/?ysclid=ly5seejcc9653928983
17. https://xakep.ru/2024/06/28/au10tix-leak/
18. https://www.darkreading.com/cyber-risk/opentext-goes-all-in-on-cybersecurity-size-and-scale-with-micro-focus-purchase
19. https://habr.com/ru/articles/825210/
20. https://www.iso.org/standard/80585.html
21. Емельянников М. Защита персональных данных в электронной коммерции//Открытые системы. СУБД. 2011. № 6. С. 30.
22. Тимерханова С.А. Система защиты персональных данных в виртуальной инфраструктуре//Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. 2018. № 1-2. С. 92-96.
23. Бундин М.В. К вопросу о монетизации персональных данных // В книге: Московский юридический форум онлайн 2020. Сборник тезисов докладов: в 4 частях. Москва, 2020. С. 162-166.
24. Щепетов В.В., Бурденко Е.В. Персональные данные в сети Интернет: общие риски и пути их минимизации // В сборнике: Экономическое развитие в XXI веке: тенденции, вызовы и перспективы. Сборник научных трудов IX Международной научно-практической конференции «Горизонты России» 23 апреля 2021 г.: в 2 ч. Российский экономический университет имени Г.В. Плеханова. 2021. С. 172-184
25. 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.
26. 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.

27. 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
28. 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.
29. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа. Вопросы кибербезопасности. – 2020. - №1 (35). – С. 42 – 51.

References:

1. https://www.securitylab.ru/news/532395.php
2. https://www.verizon.com/business/resources/reports/dbir/
3. https://www.securitylab.ru/news/536418.php
4. https://www.securitylab.ru/news/539183.php
5. https://www.securitylab.ru/news/536310.php
6. https://www.securitylab.ru/news/547531.php
7. https://www.securitylab.ru/blog/personal/achekanov/92297.php
8. https://www.forbes.com/sites/sungardas/2014/09/04/youve-completed-a-vendor-risk-assessment-now-what/
9. https://www.tarlogic.com/blog/supply-chain-attacks/
10. https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-otraslyakh-za-tri-goda
11. https://docs.cntd.ru/document/1200084141?ysclid=lwuuccw1n5461596370
12. https://docs.cntd.ru/document/1200170125?ysclid=lwuube9s8s433673326
13. https://www.rbc.ru/technology_and_media/28/05/2024/6655fc979a79477dbc9e33c4?from=from_main_2
14. https://www.cnews.ru/news/line/2024-06-10_glava_mintsifry_rossii_podderzhal
15. https://internet-law.ru/gosts/gost/73107/?ysclid=ly5sf3zra8363383699
16. ·https://internet-law.ru/gosts/gost/50679/?ysclid=ly5seejcc9653928983
17. https://xakep.ru/2024/06/28/au10tix-leak/
18. https://www.darkreading.com/cyber-risk/opentext-goes-all-in-on-cybersecurity-size-and-scale-with-micro-focus-purchase
19. https://habr.com/ru/articles/825210/
20. https://www.iso.org/standard/80585.html
21. Emelyannikov M. Personal data protection in e-commerce. *Open systems*. DBMS. 2011;6:30 (In Russ).
22. Timerkhanova S.A. Personal data protection system in virtual infrastructure. *Electronic means and control systems. Proceedings of the reports of the International scientific and practical conference.* 2018;1-2: 92-96. (In Russ).
23. Bundin M.V. On the issue of monetization of personal data.In the book: Moscow legal forum online 2020. Collection of abstracts of reports: in 4 parts. Moscow, 2020;162-166. (In Russ).
24. Shchepetov V.V., Burdenko E.V. Personal data on the Internet: common risks and ways to minimize them. In the collection: Economic development in the 21st century: trends, challenges and prospects. Collection of scientific papers of the IX International scientific and practical conference "Horizons of Russia" April 23, 2021: in 2 parts. Plekhanov Russian University of Economics. 2021:172-184(In Russ).
25. Oreshkina A.S., Livshits I.I., Sokolov E.O. Legal problems of the activities of inspectors for the protection personal data: content, features, specifics for oil and gas holding companies. *Gas industry*. 2023: 4 (847): 96-104. (In Russ).
26. Livshits I.I., Livshits M.I. Application of national standards GOST R and international standards ISO 31000 series to ensure a modern level of risk management. *Financial Risk Management.* 2022; 4.:312-323. (In Russ).
27. 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; 9: 40-56(In Russ).
28. 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;11: 50-70. (In Russ).
29. Livshits I.I. Practice of cyber risk management in oil and gas projects of holding-type companies. *Cybersecurity issues.* 2020;1 (35):42 - 51. (In Russ).

Сведения об авторе:
Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru
Information about author:
Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru
Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/ Received 18.09.2024.
Одобрена после рецензирования/Reviced 22.11.2024.
Принята в печать/Accepted for publication 20.01.2025.