УДК 004.056

Вантеев Роман Александрович,
магистрант,
Иркутский государственный университет путей и сообщений, г. Иркутск

Сачков Дмитрий Иванович,
проректор по цифровым технологиям,
Иркутский государственный университет путей и сообщений, г. Иркутск

ИДЕНТИФИКАЦИЯ И ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ НА ПОСТИНТЕГРАЦИОННОМ ЭТАПЕ ОБЪЕДИНЕНИЯ ОРГАНИЗАЦИЙ

Аннотация: *В статье рассматривается задача идентификации и оценки рисков информационной безопасности корпоративной инфраструктуры на этапе постинтеграции организаций на примере объединения крупной федеральной розничной сети поглощающей компании (далее Компания А) и региональной организации поглощаемой компании (далее Компания Б). Обоснована необходимость выделения данного этапа как самостоятельной зоны повышенного риска, поскольку в этот период одновременно действуют унаследованные уязвимости, разнородность ИТ-ландшафта, кадровая неопределенность, расширение доступа к данным и необходимость быстрого перехода к единым корпоративным процессам. Предложена прикладная модель оценки рисков, основанная на инвентаризации активов, классификации информационных систем, анализе угроз и уязвимостей, матричной оценке вероятности и ущерба, а также выборе мер обработки риска. Методика согласована с требованиями*

законодательства РФ, внутренними документами Компании Б и подходами ISO/IEC 27001, ISO/IEC 27002 и ISO/IEC 27005.

Ключевые слова: *информационная безопасность, постинтеграционный этап, корпоративная инфраструктура, объединение организаций, риск ИБ, персональные данные, коммерческая тайна, управление доступом.*

Vanteev Roman Aleksandrovich,
Graduate Student, Irkutsk State University of Railways and Communications,
Irkutsk

Sachkov Dmitry Ivanovich,
Vice-Rector for Digital Technologies,
Irkutsk State University of Railway Engineering,
Irkutsk

IDENTIFICATION AND ASSESSMENT OF INFORMATION SECURITY RISKS OF CORPORATE INFRASTRUCTURE AT THE POST-INTEGRATION STAGE OF ORGANIZATIONAL MERGER

Annotation: *The article examines the identification and assessment of information security risks in corporate infrastructure at the post-integration stage of an organizational merger, using the case of a large federal retail network (Company A) and a regional organization (Company B). The need to consider this stage as an independent high-risk area is substantiated, because inherited vulnerabilities, a heterogeneous IT landscape, personnel uncertainty, expanded access to data and the need for a rapid transition to unified corporate processes coexist during this period. The article proposes an applied risk assessment model based on asset inventory, classification of information systems, analysis of threats and vulnerabilities, matrix assessment of probability and impact, and selection of*

risk treatment measures. The methodology is aligned with the requirements of Russian legislation, internal documents of Company B, and the approaches of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005.

Keywords: *information security, post-integration stage, corporate infrastructure, organizational merger, information security risk, personal data, trade secret, access management.*

1. Введение

Постинтеграционный этап объединения организаций является одним из наиболее сложных периодов жизненного цикла корпоративной инфраструктуры. В отличие от классического внедрения информационной системы, объединение инфраструктур происходит в условиях уже работающего бизнеса, ограниченных сроков, разнородной архитектуры и необходимости обеспечить непрерывность торговых, складских, финансовых и управленческих процессов. Для розничной сети данные условия особенно критичны, поскольку нарушение доступности кассовых, учетных, логистических, кадровых и коммуникационных сервисов напрямую влияет на операционную деятельность.

В рассматриваемом кейсе Компания Б, ранее обслуживавшая магазины региональных сетей, включается в контур Компании А. На практике это означает не только юридическую и организационную трансформацию, но и постепенное приведение ИТ- и ИБ-процессов к единым корпоративным требованиям. Часть торговых объектов закрывается или переформатируется, часть продолжает работу в смешанном формате, а сотрудники, сервисы, учетные записи, каналы связи и базы данных переходят в новое состояние. Именно в этот период повышается вероятность ошибок в управлении доступом, появления «забытых» учетных записей, сохранения устаревшего программного обеспечения, неполной передачи журналов событий и неучтенного взаимодействия с подрядчиками.

Цель статьи - предложить прикладную модель идентификации и оценки рисков ИБ для корпоративной инфраструктуры на постинтеграционном этапе объединения организаций. В качестве нормативной основы используются Федеральные законы №149-ФЗ «Об информации, информационных технологиях и о защите информации», №152-ФЗ «О персональных данных», №98-ФЗ «О коммерческой тайне», Указ Президента РФ №188 «Об утверждении перечня сведений конфиденциального характера», а также внутренние документы Компании Б и международные стандарты ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 [1-8].

2. Нормативная и документальная основа оценки рисков

Для коммерческой организации базовым правовым требованием является обеспечение законности обработки и защиты информации, персональных данных, коммерческой тайны и иных сведений ограниченного доступа. Федеральный закон №149-ФЗ закрепляет общие требования к защите информации и обязанности обладателя информации принимать меры по предотвращению неправомерного доступа. Федеральный закон №152-ФЗ устанавливает требования к обработке персональных данных, включая необходимость принятия правовых, организационных и технических мер по их защите. Федеральный закон №98-ФЗ раскрывает режим коммерческой тайны как совокупность мер по ограничению доступа к сведениям, имеющим коммерческую ценность. Указ Президента РФ №188 определяет перечень сведений конфиденциального характера, что важно при разграничении категорий данных в объединяемой инфраструктуре [1-4].

Внутренняя Политика Компании Б в области информационной безопасности определяет ИБ через сохранение конфиденциальности, целостности и доступности информации, закрепляет обязательность выполнения требований для всех работников и указывает на риск-ориентированный подход как основу принятия управленческих решений в области ИБ [6]. Стандарт «Обеспечение безопасности информационных систем Компании Б» устанавливает требования к классификации ИС, учету

компонентов, взаимодействию с третьими лицами, управлению доступом, протоколированию событий, тестированию и процедуре обработки рисков при невозможности выполнить требования ИБ [7]. Отдельный документ по защите от вредоносного ПО закрепляет необходимость централизованного управления антивирусной защитой, установки АПО на серверы, АРМ и шлюзы обмена информацией, а также порядок реагирования на обнаружение вредоносного кода [8].

Таким образом, методика оценки рисков должна объединять три уровня требований: законодательный, корпоративный и прикладной. Законодательный уровень задает обязательный минимум, корпоративный - единые правила и владельцев ответственности, прикладной - конкретные технические меры в отношении ИС, учетных записей, журналов, сетевых взаимодействий и средств защиты.

Таблица 1 - Нормативная и документальная основа оценки рисков ИБ

Уровень	**Источник**	**Значение для оценки рисков**
Законодательный	149-ФЗ, 152-ФЗ, 98-ФЗ, Указ №188	Определяет обязательные требования к защите информации, персональных данных, коммерческой тайны и конфиденциальных сведений.
Корпоративный	Политика Компании Б в области ИБ	Закрепляет цели ИБ, риск-ориентированный подход, персональную ответственность, минимальность привилегий и классификацию активов.
Технический	Стандарт безопасности ИС, требования к защите от ВПО	Позволяет проверять фактическое состояние ИС: учет компонентов, доступы, журналирование, тестирование, АПО, исключения и инциденты.

Уровень	Источник	Значение для оценки рисков
Методический	ISO/IEC 27001, 27002, 27005	Задает общий цикл управления рисками: контекст, идентификация, анализ, оценка, обработка и мониторинг риска.

3. Специфика рисков ИБ на постинтеграционном этапе

Анализ профессиональных публикаций показывает, что корпоративные сделки по объединению организаций сопровождаются унаследованными киберрисками: устаревшими системами, слабыми паролями, незащищенными API, недостатками инвентаризации, отсутствием мониторинга и различиями в культуре ИБ [9]. При смене собственника также повышаются риски утечек из-за нелояльности сотрудников, падения дисциплины и потери знаний о «неочевидных» критических точках инфраструктуры [10]. Для розничной организации это проявляется в рисках утечки клиентских, кадровых, закупочных и коммерческих данных, а также в рисках нарушения доступности торговых процессов.

На постинтеграционном этапе Компания А может получить не только активы Компании Б, но и ее унаследованные проблемы: скомпрометированные системы, активные учетные записи бывших сотрудников, слабые пароли, незащищенные интеграции и разнородные средства мониторинга [9]. Для рассматриваемого кейса данная проблема усиливается масштабом. Инфраструктура Компании Б включает магазины, офисы, серверные компоненты, рабочие станции, сетевое оборудование, локальные сервисы и подрядчиков. При быстром подключении к контуру Компании А возрастает поверхность атаки и повышается риск переноса локальных проблем в более крупную инфраструктуру.

В период фактического объединения важно не только быстро установить контроль над почтой, связью и потоками данных, но и сохранить знания специалистов Компании Б, поскольку именно они могут знать скрытые зависимости и критичные узлы инфраструктуры [10]. Несовместимые

форматы, разная структура данных, дублирование систем, различия в технологической зрелости и обучение пользователей становятся самостоятельными факторами риска [12].

Отдельного внимания заслуживает защищенный обмен документами и сведениями в ходе объединения инфраструктур. Корпоративные сделки связаны с передачей конфиденциальных данных, поэтому виртуальные комнаты данных и защищенные каналы должны обеспечивать шифрование, гранулярный контроль доступа, цифровые водяные знаки и журналы аудита [11]. Для постинтеграционного этапа это означает необходимость контролировать не только производственные ИС, но и временные каналы обмена документами, проектные папки, почтовые рассылки, облачные хранилища и доступы консультантов.

4. Предлагаемая модель идентификации рисков

Для практического применения предлагается модель из шести этапов: 1) определение контекста постинтеграционного этапа; 2) инвентаризация активов и владельцев; 3) классификация ИС и данных; 4) выявление угроз, уязвимостей и существующих мер защиты; 5) количественно-качественная оценка риска; 6) выбор способа обработки риска и контроль остаточного риска. Модель не заменяет внутренние регламенты компании, а связывает их с конкретной задачей оценки рисков при объединении инфраструктур Компании А и Компании Б.

На первом этапе фиксируются границы оценки: какие магазины, офисы, ИС, серверы, каналы связи, домены, учетные записи, подрядчики и массивы данных входят в контур объединения. На втором этапе каждому активу назначаются бизнес-владелец и технический владелец, что соответствует внутреннему стандарту Компании Б, требующему определения владельцев для ИС и учета компонентов: ОС, системного имени, IP-адреса или DNS-имени, назначения компонента [7]. На третьем этапе активы классифицируются по критичности нарушения конфиденциальности, целостности и доступности.

На четвертом этапе формируется реестр угроз и уязвимостей. Для постинтеграционного этапа целесообразно выделить следующие группы: управление доступом, унаследованная инфраструктура, вредоносное ПО, сетевое взаимодействие, данные и интеграции, подрядчики, мониторинг событий, кадровые риски, физическая безопасность и соответствие требованиям законодательства. На пятом этапе применяется матрица «вероятность - ущерб», где вероятность и ущерб оцениваются по шкале от 1 до 5, а интегральный риск рассчитывается как произведение показателей. Уровень риска до 5 считается низким, 6-10 - средним, 11-15 - высоким, 16-25 - критическим.

Для учета зрелости действующих мер защиты может использоваться корректирующий коэффициент K: 1,0 - меры отсутствуют или не подтверждены; 0,8 - меры частично внедрены; 0,6 - меры внедрены и документированы; 0,4 - меры внедрены, документированы и регулярно контролируются. Тогда остаточный риск может быть рассчитан как Rост = P × I × K. Такая формула является прикладной адаптацией риск-ориентированного подхода ISO/IEC 27005 и внутренних требований Компании Б, а не универсальной государственной методикой.

Таблица 2 - Этапы модели идентификации и оценки рисков ИБ

Этап	**Содержание работ**	**Результат**
1. Контекст	Определение границ постинтеграционного этапа, критичных бизнес-процессов и участников.	Паспорт оценки рисков.
2. Активы	Инвентаризация ИС, серверов, АРМ, сетевых устройств, каналов, данных и учетных записей.	Реестр активов и владельцев.

Этап	Содержание работ	Результат
3. Классификация	Оценка критичности ИС и данных по влиянию на конфиденциальность, целостность и доступность.	Классы критичности и приоритеты проверки.
4. Угрозы	Выявление угроз, уязвимостей, слабых мест и действующих мер защиты.	Реестр сценариев риска.
5. Оценка	Расчет исходного и остаточного риска по шкале P, I и коэффициенту зрелости мер.	Карта рисков.
6. Обработка	Выбор мер: снижение, принятие, передача или избегание риска.	План мероприятий и контрольные показатели.

5. Карта ключевых рисков для постинтеграционного кейса

Ниже приведен пример укрупненной карты рисков для этапа включения инфраструктуры Компании Б в контур Компании А. Оценки являются примерными и должны уточняться по результатам фактической инвентаризации, анализа журналов, сканирования уязвимостей, интервью с владельцами процессов и проверки выполнения ВНД.

Таблица 3 - Карта ключевых рисков постинтеграционного этапа

	Сценарий риска				Меры обработки
	Сохранение активных учетных записей уволенных или переведенных			0	Сверка HR-данных с AD, отключение неактивных УЗ, запрет общих УЗ, периодическая ревизия доступов.

	Сценарий риска				Меры обработки
	сотрудников после организационных изменений.				
	Наследование слабых паролей, локальных администраторов и технологических УЗ с избыточными правами.			6	Применение парольной политики, MFA для удаленного доступа, принцип минимальных привилегий, выделенные сервисные УЗ.
	Неполный учет серверов, АРМ, сетевых устройств и локальных сервисов региональной инфраструктуры.			5	Инвентаризация компонентов ИС, назначение бизнес- и технических владельцев, ведение карточек ИС.
	Отсутствие передачи событий из части систем в корпоративный мониторинг и SIEM.			5	Единый перечень журналируемых событий, NTP-синхронизация, подключение критичных ИС к SIEM, контроль полноты логов.
	Распространение вредоносного ПО через АРМ, съемные носители или шлюзы обмена информацией.			5	Централизованное АПО, запрет отключения без согласования, проверка съемных носителей, журналирование событий АПО.
	Передача конфиденциальных документов			2	Защищенные каналы, гранулярный доступ, журналирование

	Сценарий риска				Меры обработки
	интеграционного проекта через незащищенные каналы.				операций с файлами, ограничение внешних рассылок.
	Несовместимость форматов данных и ошибки миграции справочников, остатков, кадровых или клиентских данных.			2	План миграции, тестовая среда, контроль целостности, протоколирование изменений, резервное копирование.
	Сохранение доступа подрядчиков к ИС и данным после завершения работ или изменения договоров.			2	NDA и соглашения по ИБ, реестр внешних доступов, срок действия доступов, регулярная ревизия.
	Различия в культуре ИБ и низкая осведомленность сотрудников в период изменений.			2	Обучение, тестирование знаний ВНД, коммуникации о новых правилах, контроль руководителей подразделений.
0	Подключение устаревших или неподдерживаемых систем к новой инфраструктуре без тестирования.			0	Аудит версии ПО, тестирование уязвимостей, изоляция, план вывода из эксплуатации или обновления.

6. Рекомендации по обработке и контролю рисков

Первым приоритетом является контроль идентификационной среды. Все учетные записи должны быть персонифицированы, общие учетные записи исключены, а доступы предоставлены только в минимально необходимом объеме. Для сотрудников и контрагентов, получающих доступ через Интернет, требуется двухфакторная аутентификация. Эти меры соответствуют принципам внутренней политики Компании Б о персональной ответственности, отслеживаемости действий и минимальности привилегий [6-7].

Вторым приоритетом является инвентаризация и классификация. До расширения сетевых связей с федеральной инфраструктурой необходимо подтвердить перечень активов, владельцев, IP-адресов, DNS-имен, версий ОС, назначений компонентов и статуса поддержки ПО. Неподтвержденные активы следует помещать в карантинный сегмент до прохождения проверки. Для критичных ИС должна быть подготовлена архитектурная схема, матрица ролей, перечень интеграций и перечень регистрируемых событий.

Третьим приоритетом является мониторинг. Внутренний стандарт Компании Б предусматривает протоколирование событий на серверах, сетевом оборудовании, СХД, общесистемном и прикладном ПО, системах виртуализации, СУБД и средствах защиты, а также возможность передачи логов в корпоративную SIEM [7]. На постинтеграционном этапе важно не ограничиваться формальным подключением, а контролировать полноту, качество и своевременность событий, таких как аутентификация, смена паролей, очистка журналов, создание и удаление пользователей, изменение привилегий, действия администраторов и события безопасности ОС.

Четвертым приоритетом является защита от вредоносного ПО. На серверах, АРМ и шлюзах обмена информацией должно использоваться централизованное АПО. Отключение или изменение настроек АПО допускается только по согласованной процедуре исключений, а обнаружение

вредоносного кода должно сопровождаться блокировкой, лечением или удалением зараженного файла и записью действий в журнал [8].

Пятым приоритетом является управление данными и защищенным обменом. Для интеграционного проекта следует ограничить использование незащищенной почты и открытых облачных папок, а для конфиденциальных документов применять защищенные каналы, шифрование, разграничение доступа, водяные знаки и аудит действий. Данная рекомендация согласуется с подходом к VDR и безопасным каналам взаимодействия при корпоративных сделках [11].

Шестым приоритетом является управление исключениями. Если требование ИБ невозможно выполнить без влияния на доступность ИС, риск не должен игнорироваться. Он фиксируется в реестре исключений с указанием владельца, причины, срока действия, компенсирующих мер и даты повторного пересмотра. Такой подход позволяет не блокировать бизнес-процессы, но сохранять управляемость остаточного риска.

7. Обсуждение результатов

Предложенная модель применима к ситуации, когда Компания Б уже включается в контур Компании А и находится в фазе фактического объединения инфраструктуры. Ее отличие от предварительного cyber due diligence состоит в том, что объектом анализа становится не только состояние присоединяемой компании до сделки, но и новые риски, возникающие из-за объединения доменов, сетей, политик доступа, команд сопровождения и процессов эксплуатации.

Для рассматриваемого кейса наибольшую значимость имеют риски, связанные с учетными записями, инвентаризацией, журналированием, вредоносным ПО, подрядчиками и качеством миграции данных. Эти риски не всегда проявляются как немедленный инцидент, однако именно они формируют «скрытый технический долг ИБ». Если его не устранить в первые месяцы постинтеграционного этапа, он может привести к утечкам данных,

снижению доступности сервисов, сложности расследования инцидентов и увеличению стоимости последующей модернизации.

Практическая ценность модели заключается в том, что она позволяет связать внутренние документы Компании Б с конкретной картой рисков и планом мероприятий. Например, требование о классификации ИС используется не как формальная норма, а как основание для приоритизации проверки. Требование о передаче событий в SIEM становится критерием наблюдаемости инфраструктуры. Требование о запрете эксплуатации оборудования без корректно настроенного АПО становится контролем против распространения вредоносного ПО. Такой подход делает оценку рисков проверяемой и пригодной для защиты перед руководителем или комиссией.

Заключение

Постинтеграционный этап является самостоятельным этапом управления рисками ИБ, поскольку именно в этот период совмещаются унаследованные уязвимости, разнородная инфраструктура, кадровые изменения, расширение доступов и необходимость обеспечить непрерывность бизнеса. Для коммерческой организации в РФ оценка рисков должна опираться на законодательство о защите информации, персональных данных и коммерческой тайне, а также на внутренние документы, определяющие владельцев активов, требования к ИС, управление доступом, журналирование и защиту от вредоносного ПО.

На примере Компании А и Компании Б предложена модель, включающая определение контекста, инвентаризацию, классификацию, идентификацию угроз и уязвимостей, матричную оценку риска и выбор мер обработки. Основными направлениями снижения риска являются ревизия учетных записей, инвентаризация активов, подключение критичных ИС к мониторингу, централизованная антивирусная защита, защищенный обмен интеграционными документами, контроль подрядчиков и управление исключениями. Реализация модели позволяет снизить вероятность переноса

локальных уязвимостей инфраструктуры Компании Б в контур Компании А и обеспечить управляемый переход к единым корпоративным стандартам ИБ.

Список литературы:

1. Андриянова А. Киберугрозы при слияниях и поглощениях: кто унаследует проблемы? // Computerra. 2025. 31 янв. URL: https://www.computerra.ru/307805/kiberugrozy-pri-sliyaniyah-i-pogloshheniyah-kto-unasleduet-problemy/ (дата обращения: 1.06.2026).

2. Кибербезопасность при слияниях и поглощениях: как виртуальные комнаты данных защищают конфиденциальные сделки. PowerDMARC. URL: https://powerdmarc.com/ru/ma-cybersecurity-virtual-data-rooms/ (дата обращения: 1.06.2026).

3. Петренко С.А. Методика реорганизации корпоративной системы информационной безопасности // Информационное общество. 2002. № 3. URL: http://arch.infosoc.iis.ru/emag/2002/3/5200bcb94c2d47b8c3256d57004030ce/ (дата обращения: 1.06.2026).

4. Политика Компании Б в области информационной безопасности ОБ-13-02: утв. приказом № 5 от 05.03.2026.

5. Проблемы управления данными при слияниях и поглощениях // Reddit / r/dataengineering. URL: https://www.reddit.com/r/dataengineering/comments/149yxju/data_management_challenges_in_ma/?tl=ru (дата обращения: 28.05.2026).

6. Седов О. Информационная безопасность при слияниях и поглощениях // Директор информационной службы. 2010. 5 окт. URL: https://osp.ru/cio/2010/09/13004345 (дата обращения: 28.05.2026).

7. Стандарт «Обеспечение безопасности информационных систем Компании Б» ОБ-14-02: утв. приказом № 5 от 05.03.2026.

8. Требования «Обеспечение защиты от вредоносного программного обеспечения» ОБ-11-03: утв. приказом № 5 от 05.03.2026.

9. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102046005 (дата обращения: 27.05.2026).

10. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102088094 (дата обращения: 27.05.2026).

11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264 (дата обращения: 27.05.2026).

12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261 (дата обращения: 27.05.2026).

13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

14. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls.

15. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks.