

БИЗНЕС ПОД КОНТРОЛЕМ

КАК ВЫСТРОИТЬ БЕЗОПАСНОСТЬ
И СОХРАНИТЬ УСТОЙЧИВОСТЬ
КОМПАНИИ



и
Александр Ветрогор

Александр Ветрогор

Бизнес под контролем: Как выстроить безопасность и сохранить устойчивость компании

*<https://litres.ru/74633474>
SelfPub; 2026*

Аннотация

В 8:07 пропали заказы, вскоре остановился цех, а ключевой клиент ждал отгрузку. Кто принимает решение, если данные расходятся, а ответственность размыта?

Безопасность — не набор камер и инструкций, а способность сохранить критичные процессы и восстановиться после сбоя. Книга помогает расставить приоритеты среди рисков, определить ответственных, защитить данные, деньги, людей и объекты, оценить зависимость от поставщиков и договорные обязательства. При инциденте — фиксировать факты, действовать согласованно и возвращать работу по плану.

Руководство адресовано собственникам, руководителям и специалистам по безопасности. Оно поможет увидеть уязвимости до кризиса, понять, кто и что должен делать, и проверить

готовность на практике — чтобы сбой не превращался в хаос, а компания сохраняла устойчивость.

Книга создана с помощью ИИ. Обложка: GPT Image -
Лицензия

Содержание

Безопасность бизнеса: от защиты активов к устойчивости компании	6
Карта рисков: как выявить угрозы и определить приоритеты	18
Система управления безопасностью: роли, полномочия и ответственность	33
Защита информации и цифровой инфраструктуры	47
Конец ознакомительного фрагмента.	54

Александр Ветрогор
Бизнес под контролем:
Как выстроить
безопасность и сохранить
устойчивость компании

**Бизнес под контролем: Как выстроить безопас-
ность и сохранить устойчивость компании**

Александр Ветрогор

Безопасность бизнеса: от защиты активов к устойчивости компании

В 8:07 утра экран диспетчера посерел.

— Заказов нет, — сказала она. — Вчерашние тоже не открываются.

Через двенадцать минут позвонил начальник цеха с Южной площадки: после протечки в здании отключили электричество, а электрик запретил запускать оборудование до проверки. В 8:31 на линии появился ключевой клиент. Его производственная линия ждала партию насосных модулей. Отгрузка должна была уйти сегодня.

Владелец компании «Контур-М» посмотрел на телефон, потом на сотрудников. В отделе продаж говорили, что всё заказано. На складе не были уверены, сколько готовой продукции осталось на второй площадке. ИТ-специалист обещал вернуть систему «через час», но не знал, у кого из подрядчика сейчас дежурный номер. Начальник производства считал, что цех можно открыть после осмотра, однако разрешения ещё не было.

Сигнализация была исправна. Антивирус показывал зелёный статус. В шкафу лежала папка с инструкциями. Ни один из этих фактов не отвечал на главный вопрос: **как компания выполнит обещание клиенту, если сейчас одно-**

временно недоступны система и объект?

«Контур-М» и его сотрудники — вымышленный собирательный пример. В нём нет редкой катастрофы, которая бывает раз в столетие. Есть несколько обычных сбоев, наложившихся друг на друга. Именно так часто и возникает серьёзная угроза бизнесу: не из одного громкого удара, а из слабых мест, которые по отдельности кажутся терпимыми.

Что именно нужно защищать

До этого утра владелец «Контура-М» думал о безопасности как о наборе расходов: сигнализация, антивирус, камеры, обучение и папка с правилами. Эти меры были полезны, но не складывались в ответ на вопрос, ради чего они нужны.

Ответ начинается не с техники, а с цели компании. «Контур-М» производил насосные модули и обслуживал оборудование клиентов. Его важными активами были не только станки и серверы. К ним относились данные о заказах и запасах, компетенции сотрудников, отношения с клиентами, возможность отгружать продукцию и репутация надёжного поставщика.

Актив — это то, что имеет ценность для компании или помогает ей создавать ценность. Иногда актив легко потрогать: склад, инструмент, автомобиль. Иногда он невидим: база данных, доступ к банковскому кабинету, опыт технолога, доверие заказчика. А порой самым важным активом оказывается не вещь, а способность выполнять конкретное обещание.

Чтобы увидеть, что произошло в понедельник, полезно различать несколько понятий — не ради терминологии, а ради точных решений.

Угроза — событие или обстоятельство, способное причинить ущерб: отказ системы, пожар, ошибка сотрудника, недобросовестный подрядчик, нехватка ключевой детали.

Уязвимость — слабое место, из-за которого угроза может повлиять на бизнес сильнее. Например, один человек знает, как восстановить программу, или резервная копия хранится там же и доступна через те же учётные записи, что и рабочая система.

Риск связывает возможное событие с его последствиями для целей компании. Это не просто список страшных происшествий. Отказ одной программы может быть неприятностью для отдела, но серьёзным риском для бизнеса, если без неё нельзя отгрузить товар и нет запасного способа оформить документы.

В тот понедельник компьютерная система была недоступна после сбоя при обновлении виртуального сервера. На Южной площадке протекла труба возле электрического оборудования; помещение закрыли для проверки. Причины оказались разными, но последствия сошлись на одном процессе — выполнении заказа. К этому добавились мелкие, накопленные со временем слабости: резервные копии никто не проверял восстановлением, актуального списка запасов вне системы не было, контакты подрядчика хранились у одного

сотрудника, а запасной порядок отгрузки существовал лишь в устных договорённостях.

Каждая узвимость по отдельности выглядела управляемой. Вместе они лишили руководство ясной картины и времени на решение.

Защитить объект — не значит сохранить работу

Сигнализация помогает обнаружить проникновение. Антивирус снижает вероятность некоторых компьютерных инцидентов. Инструкция может подсказать порядок действий. Но каждый инструмент закрывает лишь часть задачи, и это нормально — пока компания понимает, какую именно часть.

Безопасность снижает вероятность ущерба и ограничивает его, защищая людей, имущество, данные и операции от конкретных угроз. **Управление рисками** помогает определить, какие события важнее для целей компании, и выбрать соразмерные меры. **Непрерывность деятельности** отвечает на другой вопрос: какие критичные процессы компания должна сохранить или восстановить, если обычный порядок нарушен.

Эти направления пересекаются, но не заменяют друг друга. Хорошо защищённая система всё равно может временно выйти из строя. План непрерывности не предотвратит каждую поломку, зато поможет работать, пока специалисты восстанавливают систему. Управление рисками связывает обе задачи с реальными приоритетами компании: оно помогает не тратить одинаковые усилия на всё подряд.

Поэтому цель безопасности — не построить неприступную крепость. Абсолютной защищённости не существует, а попытка защитить всё одинаково способна истощить даже крупную компанию. Практичная цель — понять, что нельзя потерять, какие нарушения допустимы и как действовать, если защита не предотвратила сбой.

Для «Контура-М» это означало начать с клиентского обещания: отгрузить насосные модули и не оставить заказчика без информации. Из этого обещания можно выстроить понятную цепочку анализа:

Цель компании

Критичный процесс

Зависимость

Угроза

Последствие

Мера защиты и восстановления

Выполнить договор и сохранить доверие клиента

Подготовить и отгрузить насосные модули

Данные о заказе и запасах, склад, электричество, сотрудники, транспорт

Сбой системы одновременно с недоступностью основной площадки

Задержка поставки, дополнительные расходы, потеря доверия и возможные договорные последствия

Регулярно проверять восстановление данных; иметь доступный вне системы перечень заказов и запасов; предусмотреть запасную площадку или подрядчика; назначить ответственного за связь с клиентом и решение об альтернативной отгрузке

Это не теоретическая схема. Каждая её часть подсказывает следующий практический вопрос: как компания выполнит свою цель, если зависимость исчезнет или перестанет работать?

Решения под давлением

В первые минуты понедельника в «Контуре-М» все старались помочь, но каждый сообщал свою версию. ИТ-специалист ждал новостей от подрядчика, производство — разрешения вернуться в цех, отдел продаж — точных цифр со склада. Клиенту пока отвечали: «Скоро уточним».

Под давлением люди не превращаются в худшую версию себя. Но сильное напряжение сужает внимание и мешает удерживать в голове несколько версий событий одновременно. Поэтому компаниям нужны не только компетентные сотрудники, но и заранее понятный порядок: кто собирает факты, кто принимает решения, кто сообщает новости клиентам.

В «Контуре-М» владелец назначил одного координатора инцидента. Тот завёл общий список: что известно, что проверяется, кто отвечает и когда будет следующее обновление.

Руководитель ИТ занимался восстановлением системы. Начальник производства выяснял, какие безопасные альтернативы доступны. Коммерческий директор связывался с клиентом, не обещая сроков, которых компания пока не могла подтвердить.

Такое разделение не требует отдельного штаба с дорогим программным обеспечением. В небольшой компании несколькими ролями могут управлять одни и те же люди, если заранее ясно, за что каждый отвечает. Главное — не смешивать сбор фактов, принятие решений и передачу информации в бесконечный общий разговор.

К 10:30 команда выяснила, что резервная копия есть, но восстановление на чистой среде займёт несколько часов. Проверить, сколько готовой продукции находится на недоступной Южной площадке, было невозможно. Зато сотрудник сервисного центра нашёл на второй площадке шесть готовых модулей и смог сверить их с последней выгрузкой заказов. Владелец позвонил клиенту сам: шесть единиц можно отправить в тот же день, остальные — после восстановления доступа к производству. Клиенту предложили новый график, а не расплывчатое «мы разберёмся».

Компания не избежала задержки. Но она перестала терять время на противоречивые догадки и сохранила важнейшую часть обязательства: начала поставку, обозначила реальный план и поддерживала связь.

Пять шагов от защиты активов к устойчивости

Опыт «Контура-М» можно превратить в рабочий порядок для любой компании — от небольшой мастерской до крупной сети.

1. Определите, что бизнес обязан сохранить. Начните не со списка оборудования, а с нескольких целей: безопасность людей, выполнение ключевых договоров, выпуск продукции, обслуживание клиентов, соблюдение требований, доступ к деньгам и данным. Уточните, какие обязательства нельзя надолго прерывать и какие последствия задержки неприемлемы.

2. Найдите критичные процессы. Выберите действия, без которых ключевые цели не будут достигнуты: принять заказ, произвести, проверить, отгрузить, выставить счёт, обработать обращение клиента. Важно описать процесс целиком, а не только работу одного отдела. Отгрузка, например, может зависеть одновременно от производства, склада, информационной системы, перевозчика и полномочий сотрудника на оформление документов.

3. Раскройте зависимости и слабые места. Для каждого процесса спросите: какие люди, помещения, данные, подрядчики, оборудование и разрешения нужны? Что произойдёт, если исчезнет хотя бы одна зависимость? Есть ли запасной путь? Резервная копия — надёжная опора лишь тогда, когда её можно восстановить. Два экземпляра данных на одном устройстве или в одной учётной записи могут оказаться одной точкой отказа, а не резервированием.

4. Назначьте ответственных и заранее определите границы решения. У каждого важного процесса должен быть владелец, который понимает, как тот устроен и что требуется для восстановления. Отдельно договоритесь, кто руководит инцидентом, кто может изменить график или привлечь подрядчика, кто сообщает клиентам и кто проверяет безопасность людей. Без полномочий ответственный часто остаётся лишь наблюдателем.

5. Подготовьте меры предотвращения и восстановления. Меры должны соответствовать выявленному риску. Это могут быть резервное копирование и проверка восстановления, контроль доступа, техническое обслуживание, запасные компоненты, альтернативный поставщик, обучение сотрудников, бумажный порядок оформления или соглашение о резервной производственной площадке. Не каждую компанию нужно дублировать целиком. Но для критичного процесса необходимо понимать, сколько времени он может не работать и какой объём данных допустимо потерять.

Последние два ориентира часто называют временем восстановления и допустимой потерей данных. Их не следует назначать одинаковыми для всех систем. Для отдела кадров задержка доступа на день может быть переносимой; для диспетчеризации доставки несколько часов могут сразу повлиять на клиентов. Ценность ориентира в том, что он превращает абстрактное «надо быстрее восстановить» в конкретный вопрос: какой срок приемлем именно для этого процес-

са?

И ещё одно правило: меры защиты нужно проверять действием. Наличие резервной копии в отчёте не доказывает, что из неё можно восстановить сервис. Инструкция, которую никто не открывал, не гарантирует, что сотрудник сумеет выполнить её под давлением. Учебная тревога необязательно должна быть сложной: можно провести короткий разбор сценария «система недоступна, руководитель объекта не отвечает, клиент ждёт поставку» и проверить, кто принимает решения и где искать нужные сведения.

Простая проверка зрелости

Чтобы понять, с чего начать, задайте себе четыре вопроса:

1. Что именно компания защищает? Можно ли назвать несколько ключевых целей и процессов — или ответ сводится к перечню купленных устройств?

2. От чего зависит работа? Известны ли критичные сотрудники, системы, площадки и поставщики? Есть ли зависимости, о которых знает только один человек?

3. Кто принимает решения? Понимают ли сотрудники, кто руководит инцидентом и какие действия можно предпринимать без дополнительного согласования?

4. Как компания восстанавливается? Проверялись ли резервные копии, запасные процессы и контакты ответственных реальным упражнением?

Неясный ответ — не повод обвинять сотрудников или немедленно покупать ещё одну систему. Это указатель, где

сначала нужно собрать факты. Для небольшой компании достаточно начать с одного критичного процесса и одного обсуждения с руководителями. Для более сложного бизнеса работа может потребовать отдельной оценки, но принцип тот же: усилия направляют туда, где нарушение сильнее всего заденет цели компании.

Попробуйте короткое упражнение. Выберите обещание, которое важно для клиентов или финансовой устойчивости. Запишите процесс, необходимый для его выполнения, назовите главные зависимости и представьте, что одна из них пропала на сутки. Затем ответьте: кто принимает решение, какая информация ему нужна и что компания сможет предложить клиенту? Если последняя строка остаётся пустой, перед вами не обязательно катастрофа — но точно важная задача.

Следующий сбой

Через несколько месяцев у «Контура-М» пропал доступ к корпоративной сети на региональной площадке. Теперь сотрудники не стали ждать, пока кто-нибудь первым догадается, что происходит. Координатор открыл короткий порядок действий, руководитель склада сверил доступный вне системы перечень отгрузок, а коммерческий директор предупредил затронутых клиентов и назвал время следующего обновления. ИТ-команда восстановила подключение, а сотрудники внесли временные записи в систему после проверки данных.

Заминка была. Паники — нет. Самое важное: компания продолжила выполнять обязательства и знала, что будет делать дальше.

В этом и заключается переход от охраны отдельных активов к устойчивости. Сигнализация, антивирус, резервные копии и инструкции полезны не сами по себе, а как части управляемой способности: понять, что важно, принять решение под давлением, сохранить критичную работу и восстановиться после нарушения. Хорошая безопасность не обещает, что сбоя никогда не случится. Она помогает компании не потерять себя, когда привычный порядок даёт сбой.

Карта рисков: как выявить угрозы и определить приоритеты

В переговорной пахло кофе, маркерами и лёгкой паникой. На экране — таблица с заголовком «Риски». Под ним уже стояло тридцать одно слово: кибератака, уход технолога, пожар, срыв поставок, штрафы, утечка данных, поломка линии, мошенничество, скачок цен...

Компания «ТерраФуд» выпускала готовые блюда и поставляла их торговым сетям. Операционный директор постукивал ручкой по столу:

— Если не приедет упаковка, мы остановимся через неделю.

ИТ-директор возразил:

— А если зашифруют систему заказов, мы можем не понять, что и куда отгружать.

Руководитель производства добавил:

— Уйдёт наш технолог — некому будет подтвердить изменения рецептов и режимов.

Каждый говорил о реальной опасности. Но к концу часа список вырос до сорока трёх пунктов, а действий не появилось. Все спорили, что страшнее, потому что никто не договорился, **что именно компания обязана сохранить.**

Тогда генеральный директор спросил:

— Что может помешать нам выполнить главные обязательства перед клиентами, сотрудниками и законом?

Вопрос изменил разговор. Вместо каталога бед началась работа.

Не предсказывать будущее, а готовиться к нему

Карта рисков — не перечень страшных событий и не попытка угадать, что случится в следующем году. Это инструмент, который помогает увидеть, как неопределённость может повлиять на цели компании, понять, насколько организация готова, и выбрать, что делать дальше.

Угроза сама по себе ещё не является хорошо описанным риском. «Кибератака» — слишком широкая тема для решения. Руководителю нужно понимать конкретную цепочку: например, фишинговое письмо приводит к краже учётных данных; злоумышленник получает доступ к системе заказов; компания не может вовремя собирать и отгружать продукцию.

Практическая форма сценария проста:

причина — событие — последствия.

- Причина: один поставщик обеспечивает большую часть компании важным материалом.
- Событие: поставщик прекращает отгрузки из-за аварии на производстве.
- Последствия: запас упаковки заканчивается, выпуск и поставки клиентам останавливаются.

Эта цепочка дисциплинирует обсуждение. Она не утвер-

ждает, что событие обязательно произойдёт. Она позволяет спросить: какие цели оно затронет, что уже защищает компанию и где остаётся уязвимость?

Шаг первый. Определите контекст и цели

Начинать следует не с поиска угроз, а с понимания того, что бизнес должен продолжать делать. У «ТерраФуд» участники совещания выделили четыре обязательства:

1. выпускать безопасную продукцию;
2. выполнять согласованные заказы торговых сетей;
3. сохранять прослеживаемость сырья, партий и отгрузок;
4. своевременно платить сотрудникам и критически важным поставщикам.

Список не должен охватывать вообще всё. Он должен показывать, какие результаты нельзя терять без серьёзных последствий. Для каждой цели полезно установить границы: сколько времени компания может обходиться без процесса, какой объём задержек допустим, какие требования закона или договора нарушать нельзя.

Это помогает отличить неудобство от угрозы устойчивости. Если принтер в отделе продаж ломается, работа может замедлиться. Если компания теряет доступ к данным о партиях продукции, возникает уже другой масштаб последствий.

Привлекайте к разговору людей из разных функций: производство, продажи, финансы, ИТ, кадровая служба, снабжение, юристы. Руководитель видит обязательства и compro-

миссы, специалист на месте — реальные обходные пути и уязвимости. Важно, чтобы люди могли говорить о сбоях без страха быть обвинёнными: иначе карта будет отражать не действительность, а то, что безопасно произнести вслух.

Полезно заранее обозначить рамки обсуждения: рассматриваем риски на ближайшие 12 месяцев или на более долгий период? Включаем ли в карту только внутренние процессы или также поставщиков, подрядчиков и инфраструктуру? Без этих договорённостей два участника могут оценивать один риск, но говорить о разных горизонтах и масштабах.

Шаг второй. Описывайте сценарии, а не ярлыки

После определения целей можно вернуться к опасениям руководителей и превратить их в конкретные сценарии.

Сценарий первый: сбой системы заказов. Причиной может стать фишинг, компрометация учётной записи или техническая ошибка. Событие — потеря доступа к системе, где хранятся заказы и сведения об отгрузках. Последствия — задержки поставок, ошибки в документах и затруднения с прослеживаемостью продукции.

Сценарий второй: уход ключевого технолога. Причина — увольнение, болезнь или длительное отсутствие сотрудника. Событие — знания о проверке рецептур и производственных режимов оказываются недоступны. Последствия — замедление выпуска, ошибки при изменениях и повышенная нагрузка на остальных работников.

Сценарий третий: перебой у поставщика упаковки. Причина — пожар, финансовые проблемы или сбой у поставщика его сырья. Событие — компания не получает упаковку в нужном объёме. Последствия — накопление незавершённой продукции, задержки заказов и потеря выручки.

Сценарий становится полезнее, если в нём видны причина, событие и последствия, а не только название угрозы. «У нас зависимость от поставщика» — пока наблюдение. «Из-за остановки единственного одобренного поставщика упаковки компания не сможет выполнять заказы через неделю» — уже основа для решения.

Риски могут соединяться. Например, сбой ИТ затруднит поиск заменяющего поставщика, а отсутствие технолога замедлит одобрение альтернативной упаковки. Не обязательно описывать все возможные комбинации, но важно замечать зависимости, способные усилить последствия.

Шаг третий. Проверьте действующие меры и слабые места

Руководители часто считают, что компания защищена, потому что нужное средство или процедура «есть». Но наличие контроля на бумаге не равно его работоспособности.

У «ТерраФуд» были резервные копии данных. Это хорошая мера, но никто не проверял, удастся ли восстановить систему в разумный срок. Поставщиков формально было несколько, однако только один прошёл проверку и мог отгружать нужную упаковку. Технолог оставил отдельные ин-

струкции, но часть важных решений хранилась в его личных файлах и памяти.

Для каждого сценария задайте три вопроса:

- Какие меры уже снижают вероятность события или смягчают его последствия?
- Работают ли эти меры на практике и когда их проверяли?
- Что произойдёт, если мера не сработает или ответственный человек окажется недоступен?

Так обнаруживается уязвимость: не обязательно техническая дыра, а любое слабое место, из-за которого событие легче реализуется или наносит больший ущерб. Это может быть концентрация поставок у одного контрагента, отсутствие замены ключевому сотруднику, непроверенная резервная копия или полномочия, сосредоточенные у одного человека.

Полезно различать риск до мер защиты и риск, который остаётся после их учёта. Но не превращайте это различие в бухгалтерскую точность. Достаточно ясно указать: какие меры учтены, на чём основана оценка и что пока не проверено.

Шаг четвёртый. Оцените риск, не притворяясь пророком

Для первичной оценки «ТерраФуд» использовала четыре вопроса.

Насколько вероятно событие? Оценивают вероятность в заданном временном горизонте, например в течение года. Учитывают историю компании, опыт отрасли и наблю-

даемые изменения. «Такого никогда не было» — слабый аргумент, если компания ведёт наблюдения всего два года.

Насколько тяжёлыми будут последствия? Ущерб может быть не только финансовым. Он затрагивает безопасность людей, выполнение договоров, требования закона, репутацию, денежный поток и способность восстановить работу. Для компании, выпускающей пищевую продукцию, безопасность и прослеживаемость партий нельзя оценивать только через стоимость простоя.

Насколько компания уязвима? Здесь важны зависимость от одной системы или одного человека, качество действующих мер, наличие альтернатив и опыт восстановления.

Как быстро последствия станут серьёзными? Это скорость развития риска. При постепенно сокращающихся запасах есть время отреагировать — если компания следит за остатками. При потере доступа к системе в разгар отгрузки ущерб может нарастать за часы.

Для рабочих обсуждений можно использовать шкалы от 1 до 5 или словесные оценки: низкая, средняя, высокая. Но критерии должны быть общими для участников. Например, «высокая вероятность» может означать, что похожие сбои повторялись или условия для них уже сложились, а не просто «мне это кажется вполне возможным».

Числа удобны для сравнения, но опасны, когда создают иллюзию знания. Если вероятность аварии оценили как 3, а последствия как 5, умножение этих цифр не превращает

мнение в точный прогноз. Шкалы часто порядковые: разница между оценками 2 и 3 не обязательно равна разнице между 4 и 5. К тому же один и тот же итоговый балл может скрывать два разных риска: частые небольшие сбои и редкую, но разрушительную аварию.

Поэтому используйте матрицу как способ сортировки, а не как автомат, выдающий окончательное решение. Отдельно отмечайте сценарии с небольшой вероятностью, но тяжёлыми последствиями. Их нельзя незаметно прятать в среднем балле: для них может понадобиться отдельный план действий или проверка готовности.

Качественной оценки часто достаточно, чтобы решить, кто должен изучить вопрос, какие меры проверить и нужен ли план на случай сбоя. Более точные данные нужны, когда решение дорогое, последствия велики или спор упирается в конкретные предположения. Тогда ищите историю простоев, фактические сроки поставок, долю закупок у крупнейшего контрагента, результаты тестов восстановления, частоту ошибок, данные об инцидентах. Если данных мало, так и запишите: «оценка экспертная, уверенность низкая; допущение — альтернативный поставщик не сможет начать отгрузку быстрее чем за месяц».

Рабочий реестр: от обсуждения к управлению

Карта рисков должна помогать вернуться к вопросу: что известно, что решили и кто отвечает. Для этого достаточно простого реестра.

Поле

Что записать

Цель

Какое важное обязательство или результат компании затрагивается

Сценарий

Конкретная цепочка «причина — событие — последствия»

Причины

Условия и факторы, которые могут привести к событию

Последствия

Что пострадает: сроки, деньги, безопасность, закон, репутация, непрерывность

Действующие меры

Что уже снижает вероятность или ущерб и насколько это проверено

Оценка

Вероятность, последствия, уязвимость, скорость развития; уровень уверенности

Владелец

Руководитель, который отслеживает риск и организует решения

Решение

Снизить, передать, принять или избегать риск; конкретные действия

Срок пересмотра

Дата или событие, после которого оценку нужно обновить

Вот как могли бы выглядеть записи «ТерраФуд»:

● **Цель:** выполнить заказы торговых сетей. **Сценарий:** остановка единственного одобренного поставщика упаковки приводит к нехватке материала и задержке выпуска. **Причины:** высокая концентрация закупок, длительное одобрение альтернативы. **Последствия:** простой и невыполненные поставки. **Действующие меры:** запас на несколько дней, неформальные контакты с другим производителем. **Оценка:** вероятность средняя или высокая; последствия высокие; уязвимость высокая; времени на реакцию мало. **Владелец:** директор по снабжению. **Решение:** снизить. **Пересмотр:** через месяц или после испытания альтернативного поставщика.

● **Цель:** сохранять управляемость отгрузок и прослежи-

ваемость продукции. **Сценарий:** компрометация учётных данных блокирует доступ к системе заказов. **Причины:** фишинг и непроверенное восстановление из резервной копии. **Последствия:** задержки, ошибки в отгрузках, затруднение поиска информации о партиях. **Действующие меры:** резервное копирование, многофакторная аутентификация для части систем. **Оценка:** вероятность оценена с невысокой уверенностью; последствия очень высокие; скорость развития высокая. **Владелец:** ИТ-директор. **Решение:** снизить. **Пересмотр:** после теста восстановления и проверки доступа.

- **Цель:** выпускать безопасную продукцию без потери качества. **Сценарий:** уход технолога оставляет без замены знания и полномочия, необходимые для проверки изменений. **Причины:** концентрация экспертизы у одного сотрудника. **Последствия:** задержка решений и повышенный риск ошибок при перенастройке процессов. **Действующие меры:** часть инструкций сохранена, дублёр не подготовлен. **Оценка:** вероятность неизвестна; уязвимость высокая; последствия серьёзные. **Владелец:** руководитель производства. **Решение:** снизить. **Пересмотр:** после подготовки и проверки дублёра.

Оценки здесь — не готовые диагнозы и не универсальные цифры. Их смысл в том, чтобы сделать видимыми основания для решения. Если участники не согласны, записывайте, в чём именно: в вероятности, масштабе последствий или на-

дёжности существующих мер. Спор может показать, какие факты нужно собрать.

Шаг пятый. Расставьте приоритеты и выберите ответ

В первую очередь смотрите не на то, кто громче выступал на совещании, а на связь риска с целями, тяжесть последствий, уязвимость и время, которое остаётся на реакцию. Учитывайте обязательные требования закона и договоров: их нарушение может сделать риск приоритетным независимо от удобства общей шкалы.

Для каждого риска компания выбирает один из четырёх основных ответов.

Снизить. Изменить процессы, укрепить контроль, проверить резервную систему, подготовить замену специалисту, диверсифицировать поставки. Это не значит устранить риск полностью; цель — снизить вероятность, последствия или и то и другое.

Передать. Использовать страхование, договорные условия, резервного подрядчика. Передать можно часть финансовых последствий или обязательств, но не ответственность компании за всё происходящее. Страховой полис не доставит упаковку вместо остановившегося поставщика, а договор не гарантирует, что подрядчик восстановится быстрее компании.

Принять. Сознательно оставить риск на текущем уровне, потому что дальнейшие меры слишком дороги или по-

следствия укладываются в допустимые границы. Принятие — это не забыть и не надеяться на удачу. Нужны основание, уполномоченный руководитель, понимание остаточного риска и условие пересмотра.

Избегать. Отказаться от деятельности, процесса или решения, создающего недопустимый риск. Например, не запускать продукт или не подключать систему, пока не выполнены необходимые требования безопасности.

У каждой меры должны быть владелец, срок и способ проверки результата. «Улучшить кибербезопасность» — намерение. «ИТ-директор до конца месяца восстанавливает систему из резервной копии на тестовой среде и фиксирует время восстановления» — действие, которое можно проверить.

Когда карта становится планом

На следующем совещании «ТерраФуд» обсуждала уже не сорок три угрозы. На столе лежали три сценария, для каждого были названы владелец и ближайший шаг.

Директор по снабжению обязался в течение десяти дней найти альтернативного поставщика и начать проверку образцов; до её завершения компания должна определить допустимый страховой запас. ИТ-директор получил срок на тест восстановления и подготовку порядка ручной обработки заказов на случай недоступности системы. Руководитель производства должен был передать критически важные инструкции, назначить дублёра технолога и проверить, способен ли

он самостоятельно пройти ключевые процедуры.

Решения не устранили неопределённость. Но у компании появились конкретные способы проверить свою готовность. Пересмотр карты назначили после теста восстановления, проверки альтернативного поставщика и подготовки дублёра, а не просто «когда-нибудь в следующем квартале».

Попробуйте провести такое же упражнение у себя. Выберите одно важное обязательство компании. Попросите представителей трёх разных функций описать, что может мешать его выполнить. Для одного сценария заполните реестр, отметьте допущения, назовите владельца и согласуйте первый проверяемый шаг. Если в комнате возник спор, не торопитесь его заглушить: возможно, именно там спрятано различие в понимании процессов или фактах.

Хорошая карта не обещает, что плохие события не произойдут. Она помогает увидеть, где компания зависит от одного человека, поставщика или системы, какие меры существуют только на бумаге и на что необходимо направить внимание прежде всего. Когда следующий кризис начнётся не по сценарию, организация будет опираться не на самый громкий голос в переговорной, а на ясные цели, проверенные меры и заранее назначенную ответственность.

Карта рисков становится полезной в тот момент, когда после обсуждения можно ответить на три вопроса: **что мы делаем, кто за это отвечает и когда проверим результат?** А чтобы эти ответы не остались добрыми намерениями, ком-

пании нужна система управления безопасностью — с ясными ролями, полномочиями и ответственностью.

Система управления безопасностью: роли, полномочия и ответственность

В 16:42 сотрудница отдела продаж замечает, что из клиентской системы выгружается необычно большой список записей. Она сообщает руководителю. Тот пересылает письмо в ИТ: «Проверьте, пожалуйста, не ошибка ли это». ИТ видит активную учетную запись, но не понимает, можно ли её отключить: выгрузка может быть связана с важной работой отдела. Специалисты по безопасности подтверждают, что поведение нетипично, и спрашивают, кто уполномочен остановить операцию. Руководитель отдела занят на встрече. Ответственного за клиентский процесс найти не удаётся.

У каждого есть начальник. У каждого есть веская причина не принимать чужое решение. А данные продолжают уходить.

Никто не бездействует намеренно. Сотрудники сообщили о подозрении, руководитель передал информацию, ИТ проверило техническую сторону, служба безопасности оценила риск. Но компания не ответила на главный вопрос: кто вправе превратить оценку в действие? Именно здесь становится заметно различие между набором специалистов и системой управления. Специалисты могут быть опытными и добросо-

вестными, но без ясных полномочий их работа похожа на спасательную команду, у которой есть оборудование, но нет права войти в здание.

Когда ответственность ходит по кругу

Организационная схема показывает, кто кому подчиняется. Система управления показывает, кто и в каких пределах принимает решения, кто их исполняет и что происходит, если человек недоступен или ситуация выходит за рамки обычной.

Это не одно и то же. На схеме может быть директор по безопасности, руководитель ИТ и несколько владельцев процессов. Но если ни одному из них не поручено остановить подозрительную операцию, схема не поможет в момент тревоги. Она лишь подскажет, кому отправить ещё одно письмо.

В стрессовой ситуации проблема усугубляется. Внимание сужается, рабочая память перегружена, а сложный выбор требует больше времени. Когда к этому добавляется неопределённость полномочий, люди склонны ждать подтверждения, даже если понимают, что промедление опасно. В исследованиях группового поведения давно описан эффект рассеивания ответственности: если роль не назначена, каждый может предположить, что действовать должен кто-то другой. В компании этот эффект нередко выглядит не как равнодушие, а как очень вежливая цепочка согласований.

Чтобы разорвать её, нужно заранее договориться о четырёх вещах:

1. Кто решает — в том числе кто принимает остаточный риск.

2. Кто действует — кто выполняет контроль или запускает ответные меры.

3. Кто помогает — чьё мнение необходимо для качественного решения.

4. Кто отвечает за результат — кто следит, чтобы вопрос не потерялся между подразделениями.

Ответы должны быть известны не только руководителям. Их нужно закрепить, сделать доступными и проверить на практике.

Безопасность — общая функция, а не чужой отдел

Ни одна профильная служба не может в одиночку управлять всеми рисками бизнеса. Служба безопасности не знает всех нюансов клиентского процесса. ИТ не всегда вправе решать, какой перерыв в работе допустим. Юристы не могут принять коммерческий риск вместо владельца продукта. А руководитель подразделения не обязан сам разбираться в настройках технических средств, чтобы понимать последствия решения.

Работающая модель распределяет роли.

Руководство задаёт допустимый уровень риска, утверждает принципы и обеспечивает ресурсами. Оно определяет, какие последствия для компании неприемлемы: например, длительная остановка критичного сервиса, нарушение обязательств перед клиентами или утрата чувствительных

данных. Руководство может делегировать решения, но не может делегировать саму обязанность создать понятные границы.

Владелец бизнес-процесса знает, что именно нужно сохранить и чем компания рискует при остановке процесса. Он отвечает за операционное решение в пределах предоставленных полномочий и принимает остаточный риск там, где ему разрешено это делать. Если потенциальный ущерб выходит за рамки делегированного лимита, решение поднимается выше. Владельцем риска не становится автоматически тот, кто громче всех участвовал в обсуждении или последним ответил на письмо.

Профильная функция безопасности предлагает правила и методы оценки, помогает определить последствия, координирует реагирование и указывает на отклонения. Она не должна молча принимать коммерческий риск за бизнес и не может подменить владельца процесса. Её ценность — в компетентном совете, своевременной эскалации и способности удерживать общий взгляд на угрозу, когда подразделения видят лишь свою часть.

ИТ и операционные команды внедряют и поддерживают технические и организационные меры: ограничивают доступ, резервируют данные, восстанавливают сервисы, фиксируют события. Они отвечают за качество исполнения, но не обязаны в одиночку определять, какой ущерб бизнес готов принять ради непрерывности работы.

Сотрудники замечают необычное, сообщают о проблемах и выполняют известные им правила. От них нельзя требовать диагностировать атаку или самостоятельно оценивать ущерб. Их обязанность — быстро передать сигнал по доступному каналу, а обязанность компании — не дать ему исчезнуть в очереди.

Наконец, **независимая проверка** оценивает, работают ли правила на практике. Её могут выполнять внутренний аудит, контрольная функция или другой независимый от исполнителей механизм. Проверяющий не должен одновременно владеть контролем, который проверяет: иначе получается экзамен, на котором человек сам себе выставляет оценку.

Матрица, которая отвечает на практические вопросы

Простой способ распределить работу — матрица ответственности. В разных компаниях используют обозначения RACI или их варианты. Важно не название, а договорённость:

- **Владелец решения** утверждает решение и отвечает, чтобы оно было принято в срок.
- **Исполнитель** делает работу.
- **Консультируемые** дают необходимые сведения до решения.
- **Информируемые** получают информацию после него или по мере развития ситуации.

- **Независимый проверяющий** оценивает качество процесса отдельно от его исполнителей.

Для каждой конкретной развилки должен быть один ясно названный владелец решения. Если решение зависит от уровня серьёзности, заранее записывают, кому принадлежит право на каждом уровне.

Процесс

Владелец решения и результата

Исполнитель

Кого консультируют

Кого информируют

Независимая проверка

Утверждение правил безопасности

Руководство в пределах корпоративных полномочий

Служба безопасности готовит и поддерживает правила

Владельцы процессов, ИТ, юристы, HR

Руководителей и сотрудников, которых затрагивают правила

Внутренний аудит или контрольная функция

Принятие исключения из правила

Владелец процесса в пределах делегированного риска; выше установленного порога — руководитель соответствующего уровня

Владелец процесса оформляет решение и условия; профильные команды выполняют меры

Безопасность, ИТ, юристы, финансы — по характеру риска

Руководство и затронутые команды

Независимая проверка периодически оценивает исключения

Внедрение меры защиты

Владелец процесса подтверждает требование и приемлемость изменений

ИТ или назначенная операционная команда

Безопасность, пользователи, поставщик решения

Заинтересованные подразделения

Контрольная функция проверяет выбранные меры

Реагирование на подозрительную активность

Назначенный руководитель инцидента — в рамках заранее делегированных полномочий

ИТ и профильные команды локализуют проблему; владелец процесса организует работу бизнеса

Безопасность, юристы, коммуникации — по необходимости

Руководство, затронутые подразделения и другие стороны по установленным правилам

После инцидента проводится независимый разбор

Проверка восстановления и готовности
Владелец процесса отвечает за результат восстановления
ИТ и операционные команды восстанавливают сервис и
подтверждают его работоспособность
Безопасность и пользователи процесса
Руководство и зависимые подразделения
Аудит или отдельная контрольная проверка

У матрицы есть важное ограничение: она не заменяет договорённости и связь. Документ, который лежит в папке, недоступной ночью, — не механизм управления. Если в нём указана фамилия человека, ушедшего из компании полгода назад, — это уже исторический документ. Матрица полезна лишь тогда, когда люди знают, где её найти, понимают свои полномочия и могут связаться с нужным человеком.

Стоит также разделять «исполнитель» и «ответственный за результат». ИТ может выполнить техническую изоляцию, но владелец процесса должен подтвердить, что после неё бизнес способен продолжать работу безопасным способом. Служба безопасности может рекомендовать ограничить доступ, но решение о принятии серьёзного остаточного риска должно принадлежать тому уровню руководства, которому такие полномочия действительно предоставлены.

Принятие риска нельзя оформлять фразой «все согласны». Нужно записать: какой именно риск принимается, по-

чему это необходимо, на какой срок, какие меры снижают последствия, кто дал согласие и при каких условиях решение пересматривается. Молчание — не подпись, а отсутствие ответа.

Полномочия на остановку и правила эскалации

В матрице недостаточно указать, кто «участвует в реагировании». Нужно определить, кто может остановить опасную операцию, что считается достаточным основанием и кто разрешает возобновление.

Полезно разделить **право поднять тревогу, право временно приостановить действие и право принять решение о дальнейшем режиме работы**. Любой сотрудник должен иметь возможность добросовестно сообщить о подозрении без страха, что его накажут за ложную тревогу. В отдельных процессах назначенные специалисты могут получить полномочие на временное ограничение: например, приостановить массовую выгрузку или заблокировать учетную запись. А решение о возобновлении принимает заранее определённый владелец процесса совместно с нужными экспертами.

Для этого в регламенте указывают:

1. Триггеры. Какие признаки требуют немедленного сообщения или временной остановки, а какие можно передать в обычном порядке.

2. Первичный канал. Куда обращаться: номер дежурной линии, рабочий чат или система заявок. Для срочной ситу-

ации одного тикета недостаточно: канал должен позволять получить подтверждение, что сигнал принят.

3. Срок подтверждения. Например, установить разные нормативы для критического инцидента и обычного обращения. Важно заранее определить срок реакции, а не придумывать его во время инцидента.

4. Эскалацию. Если основной контакт недоступен, обращение сразу переходит заместителю или дежурной роли, а не зависает в ожидании одного человека.

5. Условия остановки и возобновления. Кто вправе применить временное ограничение, кто оценивает последствия и кто снимает его.

6. Замещение. Для каждой ключевой роли назначают заместителя с достаточными полномочиями и доступом к необходимой информации.

Разумное временное ограничение часто дешевле, чем продолжение неизвестной операции. Но остановка тоже может причинить ущерб. Поэтому решение не должно быть ни произвольным, ни парализованным: правила задают пределы, а владелец процесса и профильные специалисты оценивают конкретный контекст.

После инцидента важно выяснять не только, кто что сделал, но и почему система позволила промедлить. Если сотрудник добросовестно сообщил о подозрении, а проверка не подтвердила угрозу, это не повод обесценивать сообщение. Иначе в следующий раз человек сначала начнёт сомне-

ваться в себе — и только потом, возможно, позвонит.

Управление должно жить в календаре и бюджете

Безопасность становится частью управления не тогда, когда её раздел назван в политике, а когда она влияет на обычные решения бизнеса.

На регулярных встречах руководства и владельцев процессов полезно обсуждать не перечень угроз вообще, а конкретные вопросы: какие важные процессы зависят от одного подрядчика, где накопились исключения, кто способен остановить операцию и насколько быстро компания восстановится. Разговор должен завершаться назначенным владельцем решения и сроком, а не обещанием «взять на контроль».

Бюджетирование — ещё одна проверка серьёзности намерений. Если компания считает снижение риска важным, ресурсы на меры и обучение должны появляться в планировании, а не возникать только после инцидента. Владелец процесса объясняет, чего стоит непринятый риск; профильная функция — какие меры доступны; руководство сопоставляет затраты с возможными последствиями.

Наконец, безопасность нужно включать в изменения бизнеса. Запуск нового продукта, выход на новый рынок, приобретение компании, переход к облачному поставщику или изменение клиентского процесса создают новые зависимости и иногда меняют прежние границы риска. Вопрос «кто это утвердил?» следует задавать до запуска, а не после того, как обнаружилось, что новый сервис обрабатывает данные,

о которых никто не подумал.

Проверка модели на коротком сценарии

Вернёмся к выгрузке из клиентской системы. Теперь у компании есть заранее согласованные правила. Сотрудница сообщает о подозрительной активности через дежурный канал и сразу получает подтверждение. Дежурный специалист безопасности оценивает признаки и по установленному порогу временно приостанавливает выгрузку. ИТ проверяет учетную запись и ограничивает её доступ. Владелец клиентского процесса получает информацию и оценивает, какие операции могут пострадать. Если ограничение затрагивает критичный сервис сверх его полномочий, вопрос немедленно передают назначенному руководителю инцидента.

Подозрение не подтвердилось: выгрузку инициировал сотрудник для согласованной задачи, но использовал необычный способ. Команда фиксирует это, восстанавливает доступ после проверки и корректирует описание нормальных операций, чтобы в следующий раз отличить рабочее действие от опасного. Никто не обвиняет коллегу в лишней осторожности, а ИТ не приходится угадывать, можно ли выключить учетную запись. Скорость появилась не благодаря героизму, а благодаря заранее выданным полномочиям.

Практическая проверка для руководителя

Выберите один процесс, остановка которого заметно повредит компании: платежи, обработку заказов, клиентскую поддержку, производство или работу с чувствительной ин-

формацией. За 30–45 минут вместе с владельцем процесса, ИТ и службой безопасности ответьте на вопросы:

- Кто принимает риск, если предложенные меры не внедрены?
- Кто утверждает правила и исключения из них?
- Кто выполняет меры защиты и кто проверяет, что они работают?
- Кто вправе временно остановить опасную операцию?
- Кто разрешает её возобновить?
- Кому и как сообщают о проблеме вне рабочего времени?
- Кто замещает каждого ключевого участника?
- Что произойдёт, если основной контакт не ответит?

Затем проведите короткую репетицию: сообщите о подозрительной активности и засекуте не время «расследования», а время до понятного решения о следующем действии. Если участники начинают искать телефон нужного человека или спорить, чья это зона, обнаружен не недостаток исполнителей, а пробел в управлении.

Надёжная система безопасности не обещает, что рисков не будет. Она гарантирует, что важные решения не потеряются между подразделениями, полномочия не придётся изобретать во время кризиса, а ответственность не растворится в коллективном «мы думали, этим занимается кто-то другой». Начать можно с четырёх ясных ответов: кто решает, кто действует, кто помогает и кто отвечает за результат. Когда эти ответы известны заранее, специалисты перестают

ходить по кругу — и начинают работать как система.

Защита информации и цифровой инфраструктуры

В 9:07 утра Марина из отдела продаж не смогла войти в систему, где хранились карточки клиентов и история переговоров. До звонка заказчику оставалось двадцать минут. Она написала коллеге:

— Пришли общий пароль. Как обычно.

Пароль знал почти весь отдел. Его завели давно, когда в компании было шесть человек и один общий компьютер. Потом сотрудников стало сорок, система превратилась в рабочее место продаж, а привычка осталась. Казалось, что так быстрее. И, пока всё работало, вопрос «кто именно вошёл под этой учётной записью?» никому не мешал.

Коллега прислал пароль. Марина вошла, подготовила предложение и продолжила день. Но через час система уведомила администратора об изменении настроек доступа. Почти одновременно бухгалтерия пожаловалась, что не может открыть общую папку с договорами. Руководитель продаж заметил в CRM действия, которых не ожидал.

Никто пока не знал, что произошло. Возможно, учётные данные попали не в те руки. Возможно, изменился доступ через другое подключённое приложение. Возможно, проблема была связана с настройками или действиями пользова-

теля. Компания не могла уверенно ответить даже на более простой вопрос: кто пользовался общей учётной записью в последние дни?

Пришлось временно закрыть к ней доступ, проверить связанные системы и разобраться, какие данные могли быть затронуты. Но записи в журнале показывали действия учётной записи, а не конкретных людей. Часть сотрудников вошла с личных телефонов, часть работала с компьютеров, которые давно не обновлялись. Резервная копия важной папки существовала, однако никто не проверял, можно ли из неё быстро восстановить нужные документы.

Общий пароль был заметной слабостью. Но объяснять инцидент только им — всё равно что обвинить одну незапертую дверь, не заметив, что неизвестно, какие ключи ходят по зданию, кто ведёт журнал посетителей и где хранится запасной комплект. Цифровая безопасность редко ломается в одной точке. Обычно проблема возникает на стыке данных, доступов, привычек, технологий и неподготовленности к восстановлению.

Информация — это часть рабочего процесса

Компания хранит не просто файлы. В цифровых системах живут договорённости с клиентами, расчёты, сведения о сотрудниках, планы, коммерческие предложения, платёжные реквизиты и история решений. Одни данные можно потерять без серьёзных последствий. Другие раскрывают секреты бизнеса, создают юридические риски или останавлива-

ют работу целого подразделения.

Полезно рассматривать безопасность информации через три простых вопроса:

- **Кто должен видеть эти сведения?** Это вопрос конфиденциальности.

- **Кто может менять их и как понять, что изменение законно?** Это вопрос целостности.

- **Сможет ли компания пользоваться ими, когда это потребуется?** Это вопрос доступности.

Можно защищать данные от посторонних и всё же потерять к ним доступ из-за сбоя. Можно регулярно делать копии, но не заметить, что в системе годами лежат доступные всем зарплатные ведомости. Можно установить современную защиту, но оставить бывшему подрядчику рабочую учётную запись. Безопасность требует удерживать все три задачи одновременно.

И ещё важно помнить: цифровая инфраструктура — не только компьютеры в офисе. Это электронная почта, облачное хранилище, бухгалтерская система, телефоны сотрудников, сервис для общения с клиентами, интернет-банк и программы подрядчиков. Иногда один сервис становится ключом к другим: например, почтовый ящик помогает восстановить пароль от нескольких рабочих систем. Поэтому вопрос «где находятся данные?» нужно задавать вместе с вопросами «кто ими управляет?» и «через какие учётные записи к ним можно добраться?».

Сначала составьте карту, потом покупайте защиту

Нельзя разумно охранять то, чего организация не умеет перечислить. Начните не с выбора продукта, а с карты связей между информацией и рабочими системами. В неё не обязательно сразу включать каждую папку и каждый файл. Достаточно выявить важные для компании категории данных и системы, от которых зависят ключевые процессы.

Вот упрощённый пример:

Информация

Система

Пользователь

Доступ

Способ восстановления

Данные клиентов и история общения

CRM

Менеджеры, руководитель продаж, администратор

Менеджеры видят своих клиентов; руководитель — команду; администратор управляет настройками

Резервная копия и процедура восстановления учётных записей

Договоры и коммерческие предложения

Облачное хранилище

Продажи, юрист, руководители

Папки доступны по роли и конкретной рабочей задаче
Отдельная защищённая копия; проверка восстановления
файлов

Данные о выплатах и персонале
Бухгалтерская система
Уполномоченные сотрудники бухгалтерии, ограниченный
круг руководителей
Доступ только по служебной необходимости
Копия по установленному графику; восстановление с уча-
стием ответственного специалиста

Карта должна отвечать на пять вопросов: **какая инфор-
мация важна, в какой системе она хранится, кто ей
пользуется, какие действия ему разрешены и как вос-
становить работу после сбоя**. Назначьте владельца ин-
формации или процесса. Это не обязательно технический
специалист. Руководитель продаж лучше других понимает,
какие данные нужны для работы с клиентами; бухгалтер —
какие сведения нельзя потерять перед закрытием месяца.
ИТ-специалист помогает определить, как эти потребности
обеспечить технически.

Следующий шаг — классификация информации. Не нуж-
но создавать сложную систему из десятков уровней. Для на-
чала подойдут четыре понятные категории:

1. Открытая — сведения, которые компания готова пуб-

ликовать.

2. Внутренняя — рабочая информация, не предназначенная для свободного распространения.

3. Конфиденциальная — данные, раскрытие которых может навредить компании, клиенту или сотруднику.

4. Критичная — информация, потеря, изменение или раскрытие которой способны серьёзно нарушить работу или привести к значительным последствиям.

Категории должны подсказывать сотруднику, как обращаться с данными: где их хранить, кому отправлять, можно ли загружать в сторонний сервис и как долго сохранять. Если инструкции невозможно объяснить простыми словами, люди начнут руководствоваться привычкой — той самой, которая однажды превращает общий пароль в «нормальный порядок работы».

Требования к обработке и срокам хранения данных могут зависеть от законодательства, отрасли, договоров с клиентами и места размещения сервисов. В таких вопросах нужно сверяться с применимыми требованиями и привлекать профильных юристов или специалистов по защите данных. Универсальная таблица не заменяет правовую оценку.

Доступ должен следовать за работой человека

Основной принцип управления доступом прост: каждый человек получает только те права, которые нужны ему для конкретной работы. Не больше «на всякий случай», не навсегда и не потому, что его коллега уже имеет такие же права.

У сотрудника должна быть личная учётная запись. Тогда действия можно связать с конкретным пользователем, а при увольнении или смене роли — отозвать именно его доступ. Общие учётные записи эту связь размывают. Если без общей записи по объективным причинам не обойтись, её использование нужно ограничить, закрепить за ответственным владельцем и обеспечить журналирование действий. Это исключение, а не удобный стандарт.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.