



ТАЛИОН
ЭКСПЕРТ НЕО

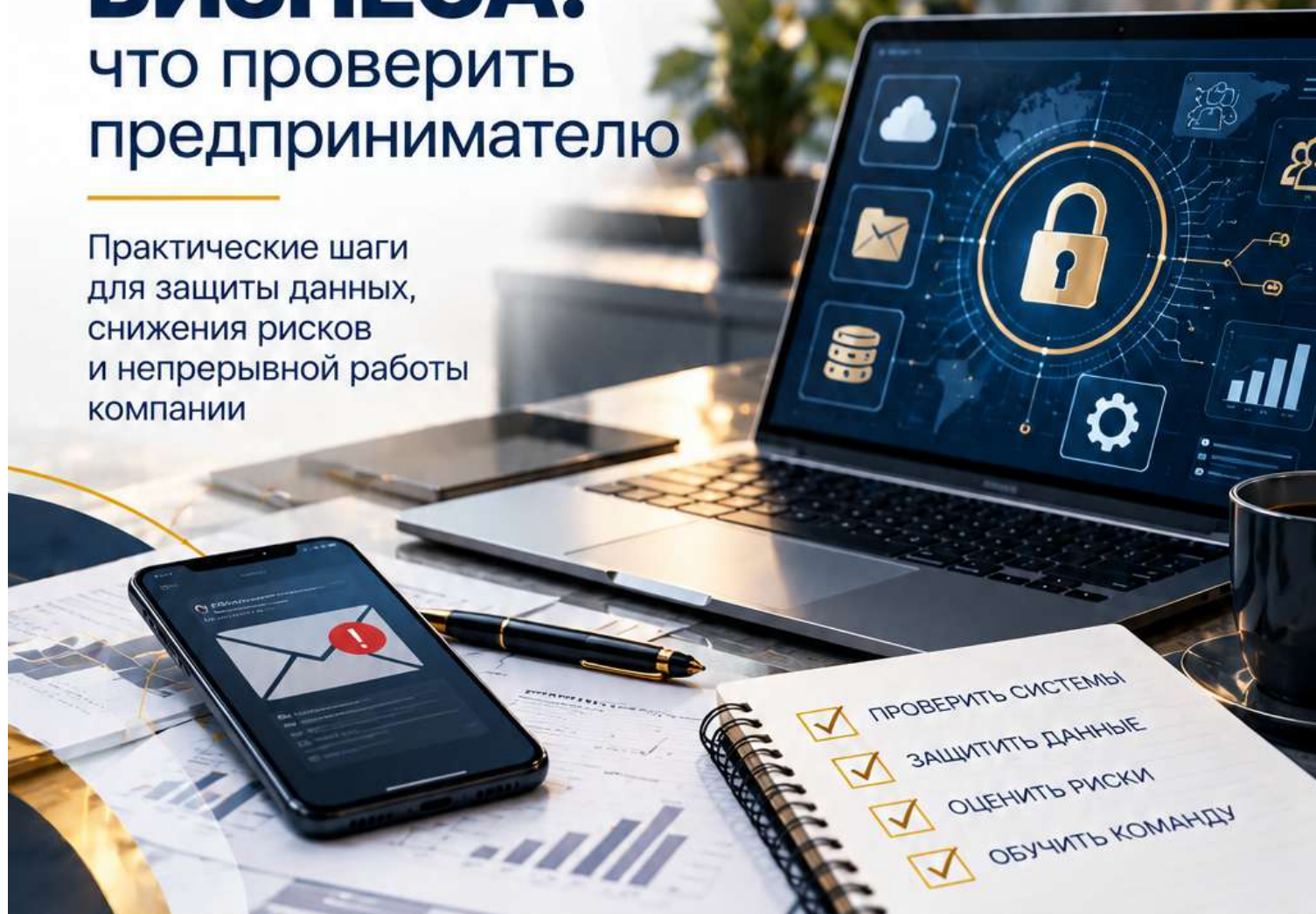
ПРАВО
ТЕХНОЛОГИИ
БЕЗОПАСНОСТЬ
ДЛЯ БИЗНЕСА

ЧЕК-ЛИСТ

ЦИФРОВАЯ БЕЗОПАСНОСТЬ БИЗНЕСА:

что проверить предпринимателю

Практические шаги
для защиты данных,
снижения рисков
и непрерывной работы
компании



ЗАЩИТА
ДАННЫХ



НЕПРЕРЫВНОСТЬ
БИЗНЕСА



УПРАВЛЕНИЕ
РИСКАМИ

ТЭН | ТАЛИОН ЭКСПЕРТ НЕО

Правовые решения
в эпоху новых технологий





ЦИФРОВАЯ БЕЗОПАСНОСТЬ: что проверить предпринимателю

Цифровая безопасность — это не только антивирус и сложные пароли. Это порядок доступа к данным, правила работы сотрудников, резервное копирование и готовность компании действовать при инциденте. Шесть пунктов ниже помогут предпринимателю проверить основные меры защиты и выявить распространённые уязвимости.

1

КОРПОРАТИВНАЯ ПОЧТА И УЧЁТНЫЕ ЗАПИСИ

- ✓ У сотрудников используются уникальные пароли, а для важных сервисов включена многофакторная аутентификация.
- ✓ Доступ к рабочим сервисам, файлам и базам данных предоставлен только тем сотрудникам, кому он необходим для работы.
- ✓ Учётные записи уволенных сотрудников и завершивших работу подрядчиков отключены или ограничены.
- ✓ Проверены способы восстановления доступа: резервная почта, телефон, секретные вопросы и контакты для сброса пароля.



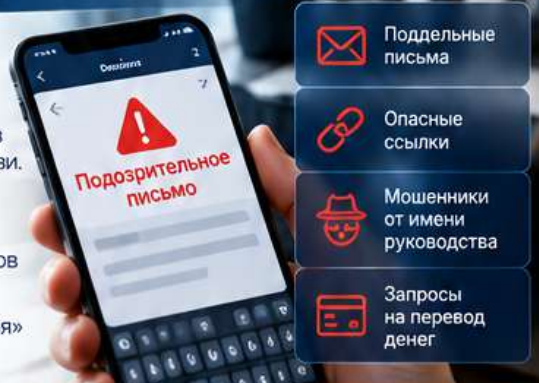
ДЕЙСТВИЕ:

Проверьте список пользователей, права доступа и способы восстановления аккаунтов. Если пароль попал к посторонним, немедленно замените его и завершите активные сессии.

2

ЗАЩИТА ОТ ФИШИНГА И МОШЕННИЧЕСТВА

- ✓ Сотрудники умеют распознавать подозрительные письма, ссылки, вложения, поддельные страницы входа и сообщения от имени руководства.
- ✓ Запросы на срочный перевод денег, изменение платёжных реквизитов или предоставление доступа проверяются по независимому каналу связи.
- ✓ Для финансовых операций установлены разные роли: сотрудник, готовящий платёж, и сотрудник, подтверждающий его.
- ✓ Передача кодов подтверждения, паролей, ключей доступа и реквизитов для входа посторонним запрещена внутренними правилами.
- ✓ Сотрудники знают, что срочность и давление со стороны «руководителя» или «контрагента» — типичные признаки мошенничества.



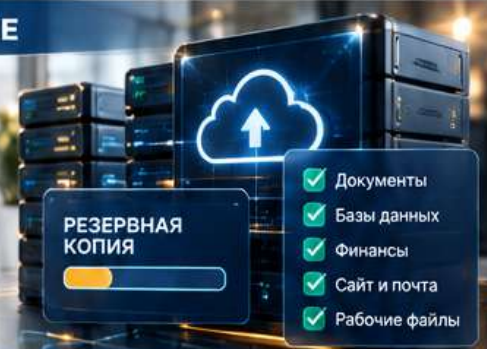
ДЕЙСТВИЕ:

Установите порядок дополнительной проверки финансовых операций. Не подтверждайте перевод денег или изменение реквизитов только на основании письма, звонка или сообщения в мессенджере.

3

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

- ✓ Важные документы, клиентские базы, финансовые данные и рабочие файлы регулярно копируются.
- ✓ Резервные копии хранятся отдельно от основных рабочих систем и защищены от случайного удаления, изменения и доступа посторонних.
- ✓ Компания проверяла, можно ли фактически восстановить данные из резервной копии.
- ✓ Определены приоритеты восстановления: какие системы и данные должны быть возвращены в работу в первую очередь.



ДЕЙСТВИЕ:

Определите периодичность копирования и ответственного сотрудника. Резервная копия полезна только если её можно использовать.



4 РАБОЧИЕ УСТРОЙСТВА И ПРОГРАММЫ

- ✓ На компьютерах, телефонах и других рабочих устройствах установлены актуальные обновления операционных систем и программ.
- ✓ Используются средства защиты от вредоносного ПО, а встроенные механизмы безопасности не отключены без необходимости.
- ✓ Установка программ, подключение внешних носителей и предоставление административных прав контролируются.
- ✓ Сотрудники не используют рабочие устройства и корпоративные аккаунты для непроверенных сервисов, личных целей или установки программ из ненадёжных источников.



ДЕЙСТВИЕ:

Составьте перечень рабочих устройств, настройте автоматические обновления и удалите ненужные программы. Ограничьте возможность самостоятельной установки программ и выдачи административных прав без необходимости.

5 ДАННЫЕ КЛИЕНТОВ И КОМПАНИИ

- ✓ Персональные данные, договоры, финансовые документы, клиентские базы и коммерческая информация доступны только уполномоченным сотрудникам.
- ✓ Общие ссылки на облачные хранилища не открывают конфиденциальные документы всем пользователям интернета.
- ✓ Перед отправкой файлов клиентам и подрядчикам проверяются адресаты, состав документов и права доступа.
- ✓ Доступ к папкам и документам периодически пересматривается, особенно после смены сотрудников, подрядчиков или структуры компании.



ДЕЙСТВИЕ:

Пересмотрите доступ к папкам, облачным хранилищам и корпоративным сервисам. Если компания обрабатывает персональные данные, проверьте соблюдение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», включая организационные и технические меры защиты.

6 ДЕЙСТВИЯ ПРИ ИНЦИДЕНТЕ

- ✓ Назначен ответственный за реагирование на взлом, утечку данных, блокировку систем и другие инциденты.
- ✓ Сотрудники знают, кому и как сообщить о подозрительной активности, потере устройства, компрометации пароля или возможной утечке.
- ✓ Предусмотрены порядок ограничения скомпрометированных доступов, сохранения доказательств, оценки последствий и восстановления работы.
- ✓ Определено, когда необходимо привлекать ИТ-специалистов, юристов, страховую компанию или правоохранительные органы.



ДЕЙСТВИЕ:

При обнаружении инцидента ограничьте скомпрометированные доступы, сохраните журналы событий, переписку и иные доказательства, оцените последствия.

Спасибо за внимание!

Этот чек-лист поможет вам безопасно и ответственно использовать цифровые технологии, снизить риски и защитить данные вашего бизнеса.

Об авторе

**Ермохина
Елена Анатольевна**



руководитель ООО «Талион Эксперт Нео»



юрист



профессиональный медиатор



лектор Общества Знаний



член Союза юристов блогеров
при АЮР



член Национальной Ассоциации
Профессиональных Медиаторов
«Паритет»

Чек-лист поможет вам



Снизить риски утечки
данных и финансовых потерь.



Наладить безопасную работу
сотрудников и подрядчиков.



Выявить уязвимости
и усилить защиту компании.



Повысить устойчивость
бизнеса к инцидентам.



Использовать цифровые
технологии с максимальной
пользой и минимальными рисками.



Цифровая безопасность — это не разовая настройка, а постоянная работа и внимание каждого, кто участвует в развитии бизнеса.