Чек-лист проверки безопасности данных

Самостоятельно анализируем безопасность и защиту данных Вашей компании.

Кратко о нас:

СОБСТВЕННЫЙ ШТАТ ВЫСОКОКВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ

ПЕРСОНАЛЬНЫЙ МЕНЕДЖЕР

12 ЛЕТ НА РЫНКЕ

ТЕХПОДДЕРЖКА 24/7

ininsys.ru
info@ininsys.ru
+7 (499) 350-28-03
117393 . , . , .43, 1

11 блоков с вопросами для базового самостоятельного аудита.

Потратив 40 минут на прохождение чек-листа, вы получите понимание, какие в вашей IT-системе уязвимости в безопасности и защите данных.

Если вы хотите получить полноценный IT-аудит с разбором состояния вашей инфраструктуры и нашими рекомендациями, то запишитесь на бесплатную диагностическую встречу по ссылке

	Да	Нет

Логины/пароли рабочих мест организации

На рабочих местах есть пароли?		
Аккаунты являются уникальными для каждого рабочего места?		
Аккаунты известны только пользователю и администратор не имеет доступа к ним?		
Пользователи имеют ограниченные учѐтные записи? (не администратор)		

Логины/пароли/телефоны почты (Yandex/mail.ru/Google)

Есть ли у организации личный почтовый сервер?		
Если сервера нет, есть ли у организации своя почта на домене (ПДД)? (вида mail@firma.ru)		
Если ПДД есть, привязан ли административный аккаунт к телефону руководителя?		
Если ПДД нет, привязана ли почта стороннего сервиса (Яндекс/mail.ru/Gmail) к телефону руководителя?		
Если ПДД нет, все ли почтовые ящики организации привязаны к корпоративным телефонам?		

Логины/пароли/телефоны соц. сетей и мессенджеров

Аккаунт vk.com организации привязан к телефону руководителя?		
Аккаунт facebook.com организации привязан к телефону руководителя?		
Аккаунт instagram.com организации привязан к телефону руководителя?		
Аккаунт tik-tok организации привязан к телефону руководителя?		
Аккаунт ok.ru организации привязан к телефону руководителя?		
Аккаунт 2gis.ru организации привязан к телефону руководителя?		
Аккаунт whatsapp организации привязан к телефону руководителя?		
Аккаунт telegram организации привязан к телефону руководителя?		
Аккаунт viber организации привязан к телефону руководителя?		

Если есть другие соц сети и мессенджеры, привязаны ли они к телефону руководителя?		

Логины/пароли/телефоны сайта (домен/хостинг/CMS)

Домен организации зарегистрирован на юр лицо или руководителя?		
Хостинг сайта оформлен на юр лицо или руководителя?		
Если сайт создан на конструкторе, этот сервис зарегистрирован на юр лицо или руководителя?		
Доступ к административной пенели сайта осуществляется по НЕ стандартному имени?		
Страница авторизации в административную панель сайта защищена от перебора паролей?		
Администатор сайта авторизовывается в системе по НЕ стандартному логину (типа admin)?		

Логины/пароли удалѐнных рабочих мест (VPN/RAT)

Каждый пользователь имеет свою личную учѐтную запись VPN?		
Множественный вход под одной учѐтной записью VPN запрещѐн?		
Есть ли ограничения для пользователей VPN на доступ к инфраструктуре?		
Запрещены ли сторонние средства удалѐнного управления (ammy admin/team viewer/anydesk)?		

Логины/пароли облачных хранилищ данных (Google/Yandex/mail.ru)

Есть ли личный сервис (Private Cloud) в организации?		
Если своего сервиса нет, учѐтная запись администратора Яндекс.Диск/Google Drive/Облако mail.ru привязана к телефону руководителя?		
Каждый сотрудник имеет личное пространство в облачном хранилище?		
Осуществляется ли резервное копирование файлов облачного хранилища?		

Логины/пароли локальных хранилищ (SMB/FTP/WebDAV)

В организации есть локальное хранилище файлов?		
Если хранилище есть, у каждого пользователя организовано личное пространство для файлов?		
Если хранилище есть, но разграничений пространства нет, есть ли ограничение на удаление файлов или иной контроль?		
Осуществляется ли резервное копирование файлов хранилища?		

Организована ли отказоустойчивость файлового хранилища?		

Логины/пароли виртуальной/локальной АТС (МТС/Билайн/etc.)

Есть ли в организации собственная АТС?		
Если собственной АТС нет, зарегистрирована ли вАТС на юр лицо или руководителя, вместе с телефонными номерами?		

Контроль и хранение

Пользователи хранят документы на сервере?		
Если пользователи хранят документы на локальном АРМ, есть ли копии на случай выхода из строя любого АРМ?		
Если пользователи хранят документы на сервере, есть ли копии любых данных на случай непреднамеренной потери?		
База 1С хранится на сервере?		
Если база 1С хранится на ПК бухгалтера, есть ли ежедневная копия, на случай еѐ повреждения/утраты?		
База клиентов хранится в CRM?		
Если база клиентов хранится в общем доступе или ПК сотрудника (не в CRM), есть ли еѐ ежедневная резервная копия?		
Контролируется ли состояние жестких дисков в серверах?		
Есть ли ответственный за выход из строя сервера и восстановление его работы?		
Контролируется ли состояние аккумуляторов в ИБП?		
Есть ли ответственный, который мониторит состояние ИБП и превентивно меняет АКБ?		
Проверяется ли валидность резервных копий?		
Есть ли ответственный, который каждую неделю контролирует состояние систем резервирования?		
Контролируется ли установка обновлений на доступные из вне серверы?		
Контролируется ли установка обновлений на доступные из вне сайты?		
Контролируется ли установка обновлений на доступные из вне маршрутизаторы?		
Контролируется ли установка обновлений на доступные из вне точки доступа?		
Изолированы ли Wi-Fi сети от приватного участка корпоративной сети?		

Сколько стоит простой?

Рассчитали стоимость выхода из строя АРМ рядового сотрудника?		
Рассчитали стоимость выхода из строя АРМ сотрудника отдела продаж?		
Рассчитали стоимость выхода из строя АРМ бухгалтера?		
Рассчитали стоимость выхода из строя АРМ главбуха/директора?		
Рассчитали стоимость выхода из строя сайта?		
Рассчитали стоимость выхода из строя сервера файлового хранилища?		
Рассчитали стоимость выхода из строя сервера производственной системы (ERP/etc)?		

Политика резервного копирования

Описаны ли точно данные, которые резервируются (что, откуда, куда, как, как часто, сколько)?		
Обеспечена ли защита от выхода из строя серверной платформы? (в отношении каждой единицы техники)		
Обеспечена ли защита от выхода из строя загрузочного диска сервера? (в отношении каждой единицы техники)		
Обеспечена ли защита от выхода из строя диска с данными на сервере? (в отношении каждой единицы техники)		
Обеспечена ли защита от намеренного/случайного удаления файлов на АРМ?		
Обеспечена ли защита от проникновения в локальную сеть вируса-шифровальщика?		
Обеспечена ли защита от одновременного выхода из строя АРМ и одного диска с данными на сервере?		
Обеспечена ли защита от одновременного выхода из строя АРМ и двух дисков с данными на сервере?		

Сколько пунктов набрали «Нет»? Если больше 25%, то это свидетельствует о структурных проблемах с безопасностью в Вашей IT-инфраструктуре.

Если вы хотите получить полноценный IT-аудит с разбором состояния вашей инфраструктуры и нашими рекомендациями, то запишитесь на бесплатную диагностическую встречу по ссылке

Преимущества работы с нами

01 Сокращаются затраты на обслуживание ИТ-инфраструктуры, в том числе на зарплату и налоги штатных сотрудников.

02 Вы не беспокоитесь, что сотрудник заболеет или уйдет в отпуск.

03 С вами работают разнопрофильные специалисты, поэтому в вашей ИТ-инфраструктуре нет уязвимых мест.

04 Вы получаете комплексное обслуживание «под ключ», без необходимости дополнительно оплачивать каждую задачу.

05 Мы приводим в порядок всё ваше оборудование и программное обеспечение.

06 Вы взаимодействуете напрямую с компетентным специалистом, без промежуточной связи с оператором и объяснением своей проблемы несколько раз.

07 Ваши данные в полной безопасности и сохранности.

08 Вы получаете бесплатный стартовый аудит, который позволяет понять структуру и проблемы вашей ИТ-инфраструктуры

09 Мы устраняем подавляющее большинство ошибок и неисправностей удаленно и быстро.

10 Мы несём финансовые гарантии качества нашей работы.

11 Мы экономим ваше время и деньги.

Более половины наших клиентов пришли к нам по рекомендации!