Памятка по кибербезопасности для контрагентов

Мы работаем с вами как партнёры. Часть нашей совместной работы происходит в интернете: обмен документами, доступ к системам, переписка. И здесь очень важно, чтобы и вы, и мы соблюдали правила кибербезопасности.

Эта памятка — не для ИТ-специалистов, а для руководителей и сотрудников вашей компании. Простые шаги помогут избежать утечек данных, взломов и финансовых потерь.

Базовые правила для компании

1. Обращайте внимание на то, что публикуете о компании и её сотрудниках в сети

Перед постом в соцсетях, новостью на сайте или фото с рабочего места спросите себя:

- Не видно ли на фото внутренние документы, пропуски в офис, экраны с рабочими данными?
- Не пишете ли вы о том, что кто-то из коллег в командировке или что офис пустует?
- Не нарушаете ли вы договор о конфиденциальности?

Если хоть на один вопрос ответили «да» — не публикуйте.

2. Знайте, какие данные вы собираете и защищайте их по-разному

У каждой компании есть:

- публичная информация (адрес, телефон, кто директор) — доступна всем;
- рабочая информация (внутренние отчёты, списки контрагентов) — доступ только у сотрудников;
- конфиденциальная информация (данные клиентов, пароли, банковские реквизиты) — должна быть под строжайшей защитой.

Проведите простую инвентаризацию: что у вас есть и как вы это защищаете.

3. Включите двухфакторную аутентификацию везде, где это возможно

Что это? После того как ввели пароль, система просит подтверждение: код из СМС, отпечаток пальца или подтверждение в приложении.

Это защищает от взлома, даже если пароль украли.

4. Установите на свой сайт SSL-сертификат (значок замка)

Зачем? Он шифрует всё, что передают пользователи на ваш сайт (например, данные из форм заявок). И он доказывает, что сайт — действительно ваш, а не подделка мошенников.

Без замка в адресной строке клиенты и партнёры не будут вам доверять.

Памятка по кибербезопасности для контрагентов

5. Пароли: длинные, сложные, разные и нигде не зафиксированы

- длина — от 12 символов;
- используйте цифры, большие и маленькие буквы, символы (!@#$%);
- не используйте целые слова (даже русские, набранные английскими буквами);
- для каждого сервиса — свой пароль;
- не передавайте пароли в мессенджерах и по почте (если только вы не шифруете письма).

Совет: используйте корпоративный менеджер паролей.

6. Обновляйте программное обеспечение

Обновления не только добавляют новые кнопки. Они закрывают дыры в безопасности, которые нашли хакеры. Чем дольше тянете с обновлением — тем больше риск, что вашу систему взломают через старую уязвимость.

Если программу нельзя обновить (старое оборудование), придумайте, как её изолировать от остальной сети.

7. Антивирус — обязателен и должен обновляться каждый день

Каждый день появляются сотни новых вирусов. Антивирус со свежими базами умеет их распознавать. Современные антивирусы ловят вирусы по их поведению — это помогает, даже если базы ещё не обновились.

8. Делайте резервные копии важных данных

Храните копии в двух разных местах: например, на внешнем диске (если это разрешено) и в облачном хранилище (облако от вашего провайдера). Если один носитель выйдет из строя или вирус зашифрует файлы — вы всё восстановите.

9. Настройте межсетевой экран (файервол) на границе вашей сети

Что это? Это “шлюз”, который решает, кому можно входить в вашу корпоративную сеть, а кому - нет. Он блокирует подозрительный трафик.

Настройте правила: какой трафик разрешён, какой запрещён. И не забывайте обновлять сам межсетевой экран.

Культура кибербезопасности внутри компании

1. Установите правила использования личных телефонов и ноутбуков для работы

Сотрудникам удобно работать с личного устройства. Но оно может быть не защищено антивирусом, или сотрудник может подключиться к опасному Wi-Fi в кафе, и тогда у хакера появится возможность получить доступ к вашей корпоративной сети.

Памятка по кибербезопасности для контрагентов

2. Разработайте план действий на случай кибератаки

Абсолютной защиты не бывает. Важно быть готовым и чётко понимать: кто принимает решения, кто отключает серверы, кто предупреждает клиентов и партнёров, кто вызывает полицию.

Назначьте ответственных и раз в полгода проверяйте, помнят ли они, что делать.

3. Обучите сотрудников правилам кибербезопасности

- Как придумывать надёжные пароли;
- Почему нельзя записывать пароли на стикерах и хранить под клавиатурой?
- Почему нельзя пересылать документы в мессенджерах (Telegram, WhatsApp и тд) и по личной почте? Какие риски это несёт?
- Почему рабочие пароли нельзя использовать для личных аккаунтов?

4. Научите сотрудников проверять значок замка (HTTPS) перед вводом любых данных на сайте

Перед тем как ввести на сайте логин, пароль или данные клиента — посмотрите в адресную строку: если там нет закрытого замка — не вводите, значит, соединение не защищено, и мошенники могут перехватить данные.

5. Руководители должны подавать пример

Если генеральный директор использует пароль «123456» и отключает двухфакторную аутентификацию — вся компания будет делать так же. Безопасность начинается с первых лиц.

6. Проведите тренинг по фишинговым письмам

Фишинг — это письма, которые выглядят как настоящие (от банка, от госорганов, от вашего директора), но на самом деле ведут на сайт мошенников или содержат вирус.

Обучите сотрудников:

- не переходить по ссылкам из подозрительных писем;
- проверять адрес отправителя по буквам;
- с осторожностью открывать вложения;
- с осторожностью открывать вложения.

7. Проводите киберучения — как минимум тренировочные фишинговые атаки на своих сотрудников

Отправьте отделу закупок письмо «от поставщика» со ссылкой на фальшивый счёт. Посмотрите, кто перейдёт. А потом проведите обучение и повторите. Так вы поймёте, насколько сотрудники готовы к реальной атаке

Памятка по кибербезопасности для контрагентов

Что делать, если атака уже произошла

1. Соберите группу быстрого реагирования

В неё входят: ИТ-специалист (отключает систему), юрист (оценивает риски), пиар-менеджер (объясняет клиентам, если данные утекли), руководитель (принимает решения). У этой группы должен быть чёткий план и право действовать без дополнительных согласований.

2. Проанализируйте, кто и как может атаковать вашу компанию

- Что самое ценное для взлома? (база клиентов, доступ к счетам, конструкторская документация)
- Кто может быть заинтересован? (конкуренты, бывшие сотрудники, хакеры «просто так»)
- Где самые слабые места? (старый сервер, сотрудник, который любит переходить по ссылкам)

Это называется **моделированием угроз**.

3. Напишите простую инструкцию для всех сотрудников на случай атаки

Пример:

1. Заметили странное (всплывающие окна, шифрование файлов, пропажу данных) — НИЧЕГО НЕ НАЖИМАЙТЕ.
2. Сообщите ответственному.
3. Не пытайтесь ничего самостоятельно исправить.

Разошлите эту инструкцию каждому сотруднику.

4. Анализируйте прошлые инциденты

Если у вас уже была утечка или вирус — после восстановления работы обязательно разберите, что пошло не так, залатайте дыру и обновите план действий. Изучайте также истории взломов других компаний в вашей отрасли — очень полезно.

5. Помните, что уязвимости есть всегда

Даже если вы купили самое дорогое оборудование и наняли лучших специалистов — абсолютной защиты не бывает. Помните, что злоумышленники каждый день находят новые уязвимости и способы обхода защиты, поэтому регулярно учитесь, анализируйте и будьте готовы действовать.

Дополнительные меры (для более серьёзной защиты)

1. Застрахуйте IT-инфраструктуру (киберстрахование)

Это полис, который покрывает убытки от кибератак: от кражи денег до восстановления данных после вируса-шифровальщика. Для малого и среднего бизнеса это может быть недорого, но очень полезно.

Памятка по кибербезопасности для контрагентов

2. Не забывайте про Интернет вещей (IoT)

Что это? Умные колонки, видеокамеры, датчики температуры, принтеры, подключённые к интернету. Они тоже могут стать точкой входа для хакера.

Правило: у каждого такого устройства должен быть уникальный пароль, и оно должно проходить проверку перед подключением к вашей основной сети.

3. Ограничьте доступ к системам. Используйте многофакторную аутентификацию не только при входе, но и для каждого важного действия

Сделайте так, чтобы даже внутри сети не все имели доступ к администрированию. Только специально назначенные люди. И только после подтверждения через второй фактор.

4. Проводите тесты на проникновение (приглашайте «белых хакеров»)

Белые хакеры — это специалисты по безопасности, которые с вашего разрешения пытаются взломать вашу систему. Они не крадут данные, а находят уязвимости и подробно отчитываются о них. Проводить такие тесты желательно раз в год или после серьёзных изменений в IT.

5. Облачные сервисы — хороший вариант для малого бизнеса

Передать данные в облако крупного провайдера часто надёжнее, чем хранить их у себя на старом сервере. Но перед этим проверьте:

- Где физически находятся дата-центры? (в России?)
- Кто имеет доступ к вашим данным?
- Как вы можете их оттуда забрать в любой момент?

Для наиболее устойчивых систем

1. Разделите вашу сеть на сегменты

Не давайте одному вирусу возможность пройти по всем компьютерам сразу. Отделите бухгалтерию от отдела продаж, серверы — от рабочих станций. Если хакер проникнет в один сегмент, он не доберётся до другого.

2. Ориентируйтесь на отраслевые стандарты, но старайтесь быть лучше

В каждой отрасли (финансы, медицина, торговля, производство) есть свои требования по кибербезопасности. Изучите их и постарайтесь выполнять чуть больше, чем требуется. Это снизит ваши риски.

3. Постоянно учитесь новому

Подходы к защите меняются каждый месяц. Подпишитесь на рассылку, раз в квартал читайте обзор новых уязвимостей, посещайте бесплатные вебинары. Не обязательно становиться экспертом, но быть в курсе — полезно.

Памятка по кибербезопасности для контрагентов

Если вы обнаружили инцидент при взаимодействии с нами

Если вы заподозрили кибератаку, которая может затронуть нашу совместную работу (например, взломан ящик для обмена документами или украдены пароли от нашего портала), немедленно сообщите нам по адресу:

- **cs-bp@sberanalytics.ru**
- **soc@sber2b.ru**

Мы разберёмся вместе и минимизируем последствия.

Кибербезопасность — это не волшебная кнопка, а привычки и простые действия. Чем больше таких привычек станут обычными для ваших сотрудников, тем спокойнее будет вам и вашим партнёрам (включая нас).

Берегите себя и свой бизнес.

С уважением и заботой,

Дирекция по кибербезопасности Сбер2В