

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ КОНТРОЛЬНЫЙ СПИСОК ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ОРГАНИЗАЦИИ

РАЗРАБОТКА ПРОГРАММЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ РИСКОВ

- Определите и составьте список всех типов информации, хранящейся или используемой в организации (например, имена клиентов и электронные письма).
- Задайте вопросы и запишите ответы для каждого типа информации:
 - Что произойдет, если эта информация будет обнародована?
 - Что произойдет с моим бизнесом, если эта информация окажется неверной?
 - Что произойдет с моим бизнесом, если я или мои клиенты не смогут получить доступ к этой информации?
- [Определите, какие технологические средства](#) будут использоваться для обработки определенной вами информации. Это может быть аппаратное обеспечение (например, компьютеры) и программные приложения (например, электронная почта в браузере).
 - При необходимости используйте технологические средства вне вашего бизнеса (например, «облачные хранилища») и любые имеющиеся инструменты защиты, например, брандмауэры.
 - Укажите марку, модель, серийные номера и другие идентификаторы.
 - Отслеживайте, где находится каждый продукт. Для программного обеспечения определите, на какие машины оно было загружено.
- Регулярно просматривайте информацию от национальных центров CERT, FS-ISAC, местного подразделения InfraGard и других организаций по угрозам и уязвимостям, возникающим в финансовом секторе, и оценивайте вероятность их возникновения у вас.
- Не реже одного раза в год проводите анализ или проверку на наличие уязвимостей.
- Разработайте политику кибербезопасности для организации.
- Уведомите всех сотрудников о политике и попросите их подписать документы, подтверждающие их роль в постоянном обеспечении кибербезопасности в вашей организации в соответствии с положениями политики.

ПРЕДОТВРАЩЕНИЕ УЩЕРБА ОТ ВРЕДОНОСНОГО ПО

- Активируйте брандмауэр и установите списки контроля доступа (ACL). Ограничьте доступ за счет внедрения списка разрешенных приложений.
- [Используйте антивирусное ПО и антишпионские программы](#) на всех компьютерах и ноутбуках.
- [Применяйте последние обновления ПО](#), предоставляемые разработчиками и поставщиками. По возможности активируйте функцию автоматического обновления.
- Убедитесь, что права на установку новых программ имеются только у ИТ-персонала с правами администратора.
- Обеспечьте ведение и мониторинг журналов активности аппаратным или программным обеспечением для защиты или обнаружения. Обеспечьте защиту журналов с помощью паролей и шифрования.
- Обеспечьте синхронизацию времени на всех хостах.

- Обеспечьте контроль доступа к съемным носителям, таким как SD-карты и USB-накопители. Вместо этого, поощряйте передачу сотрудниками файлов по электронной почте или через облачные хранилища. Информировать сотрудников о рисках использования [USB-накопителей](#) из внешних источников или передачи их USB-накопителей другим лицам.
- [Выполните настройку безопасности электронной почты и фильтров спама](#) в сервисах электронной почты.
- Обеспечьте защиту всех страниц на [общедоступных веб-сайтах](#) с помощью [шифрования](#) и других доступных инструментов.
- Рассмотрите возможность найма службы проверки на проникновение для оценки безопасности активов и систем организации.

ОБУЧЕНИЕ СОТРУДНИКОВ

- Запланируйте проведение обязательных курсов обучения по кибербезопасности во время адаптации всех новых сотрудников и через регулярные промежутки времени для текущих сотрудников (не реже одного раза в год). Требуйте от сотрудников:
 - [использовать надежные пароли](#) для всех профессиональных устройств и учетных записей, а также аналогичным образом защищать личные устройства и использовать диспетчер паролей;
 - своевременно обновлять все операционные системы, ПО и приложения [на всех](#) устройствах;
 - [использовать двухфакторную аутентификацию](#) для всех учетных записей;
 - хранить данные учетных записей и карт доступа в надежном месте и блокировать оставленные без присмотра устройства;
 - не обмениваться учетными данными или другой конфиденциальной информацией посредством незашифрованных электронных писем или других открытых сообщений;
 - [не открывать вложения](#) сразу же при получении и не переходить по ссылкам в нежелательных или подозрительных электронных письмах;
 - проверять достоверность подозрительных электронных писем или всплывающих окон перед предоставлением личной информации и обращать особое внимание на адрес электронной почты;
 - сообщать о любых потенциальных внутренних или внешних инцидентах в области безопасности, угрозах или неправильном обращении с данными или устройствами техническим специалистам организации и/или высшему руководству.
- Запланируйте и внедрите регулярную проверку осведомленности сотрудников посредством симуляции, имитируя рассылку фишинговых электронных писем с фиктивных учетных записей. Оценивайте все ненадлежащие действия сотрудников и используйте их в качестве возможностей для обучения и улучшения ситуации.

ЗАЩИТА ДАННЫХ

- [Выполняйте регулярное резервное копирование](#) важных данных (например, документов, электронных писем, календарей) и проверяйте возможность их восстановления. Рассмотрите возможность резервного копирования данных в облачное хранилище.
- Убедитесь, что устройство, содержащее резервную копию, не остается постоянно подключенным к содержащему оригиналу устройству ни физически, ни по локальной сети.
- Установите стабилизаторы напряжения, используйте генераторы и убедитесь, что все компьютеры и критические сетевые устройства подключены к источникам бесперебойного питания.
- Используйте решения для управления мобильными устройствами (MDM).

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УСТРОЙСТВ

- Включите защиту с помощью паролей или ПИН-кодов для мобильных устройств. Настройте устройства так, чтобы в случае утери или кражи с них можно было удаленно стереть данные или заблокировать.
- Своевременно обновляйте устройства (и все установленные приложения), [по возможности](#) используя функцию автоматического обновления.
- При отправке конфиденциальных данных не подключайтесь к общедоступным точкам доступа Wi-Fi, а используйте сотовые соединения (включая проводное соединение и беспроводные модемы) или используйте VPN.
- Замените устройства, которые больше не поддерживаются производителями, на более современные альтернативы.
- Разработайте процедуры отчетности о потерянном или украденном оборудовании.

ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ

- Убедитесь, что на всех компьютерах используются продукты шифрования, для загрузки которых требуется пароль. Включите защиту с помощью паролей или ПИН-кодов для мобильных устройств.
- [Используйте надежные пароли](#), избегайте предсказуемых паролей (например, passw0rd) и личных идентификаторов (таких как имена родственников и домашних животных). Проследите, чтобы все сотрудники соблюдали эти правила.
- [По возможности используйте двухфакторную аутентификацию](#) (2FA).
- Измените пароли, установленные производителем по умолчанию на всех устройствах, включая сетевые устройства и устройства «Интернета вещей», до их передачи персоналу.
- Убедитесь, что сотрудники могут быстро изменить свои пароли. Вы также можете потребовать, чтобы сотрудники регулярно меняли свои пароли (например, ежеквартально, раз в полгода или ежегодно).
- Рассмотрите возможность использования [диспетчера паролей](#). Если он уже используется, то убедитесь в надежности «основного» пароля (который обеспечивает доступ ко всем остальным паролям).

УПРАВЛЕНИЕ РАЗРЕШЕНИЯМИ

- Убедитесь, что все сотрудники имеют уникальные, идентифицируемые учетные записи, проходящие проверку при каждом доступе к системам.
- Предоставляйте административные полномочия только доверенным ИТ-сотрудникам и ключевым сотрудникам и аннулируйте права администратора на рабочих станциях для стандартных пользователей.
- Предоставляйте сотрудникам доступ к конкретным системам обработки данных только в случае необходимости для работы и убедитесь, что они не могут устанавливать ПО без разрешения.
- Создайте учетные записи для каждого сотрудника, имеющего доступ к компьютерам организации.

ЗАЩИТА WI-FI

- Убедитесь, что Wi-Fi на рабочем месте надежно защищен и зашифрован с помощью WPA2. Маршрутизаторы часто поставляются с выключенным шифрованием, поэтому обязательно включите его. Пароль защищает доступ к маршрутизатору и обеспечивает обновление пароля из предустановленного значения по умолчанию. Отключите все функции удаленного управления.
- Настройте беспроводную точку доступа или маршрутизатор, чтобы он не передавал сетевое имя, известное как идентификатор набора служб (SSID).
- Ограничьте доступ к сети Wi-Fi, разрешая доступ только устройствам с определенными адресами контроля доступа к сети. Настройте отдельную общедоступную сеть Wi-Fi для клиентов.
- Активируйте вход через протокол динамической конфигурации хоста (DHCP) на сетевом устройстве, чтобы обеспечить простое отслеживание всех входящих в сеть устройств.
- После настройки маршрутизатора выйдите из системы как администратор.
- Регулярно обновляйте ПО маршрутизатора. Зарегистрируйте маршрутизатор на сайте производителя и подпишитесь на получение обновлений.

ПРЕДОТВРАЩЕНИЕ ФИШИНГОВЫХ АТАК

- Убедитесь, что персонал не просматривает веб-страницы или не проверяет электронную почту на серверах или с учетной записи с правами администратора.
- Настройте веб-фильтр и фильтр электронной почты. Рассмотрите возможность запрета посещения сотрудниками веб-сайтов, которые обычно связаны с угрозами кибербезопасности.
- Обучайте сотрудников способам проверки наличия [явных признаков фишинга](#), таких как орфографические и грамматические ошибки, а также низкокачественные версии узнаваемых логотипов. Выглядит ли адрес электронной почты отправителя законным?
- Выполняйте сканирование на наличие вредоносных программ и изменение паролей в ближайшее время после появления подозрения об атаке. Не наказывайте сотрудников, если они стали жертвой фишинговой атаки (это приведет к тому, что в будущем они могут не сообщить вам о таком происшествии).