

# КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

## КОНТРОЛЬНЫЙ СПИСОК СОВЕТА ДИРЕКТОРОВ: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

---

### ОСНОВЫ УПРАВЛЕНИЯ КИБЕРРИСКАМИ

- Регулярно проверяйте в составе группы, может ли совет директоров утвердительно ответить на следующие вопросы:
  - Соответствует ли ваша организация применимым законодательным и нормативным требованиям, таким как Общий регламент по защите данных (GDPR)?
  - Выполнила ли ваша организация количественную оценку киберрисков и проверку финансовой устойчивости?
  - Имеет ли ваша организация действующий план по улучшению, гарантирующий, что воздействие находится в приемлемых пределах рисков?
  - Регулярно ли совет директоров обсуждает лаконичную, четкую и действенную информацию касательно предоставляемой руководством устойчивости организации к угрозам кибербезопасности?
  - Имеет ли ваша организация планы реагирования на недавно протестированные инциденты, в том числе на уровне совета директоров?
  - Являются ли роли ключевых сотрудников, ответственных за управление киберрисками, четкими и согласованным с тремя линиями защиты?
  - Получили ли вы независимую аттестацию и гарантию устойчивости вашей организации к киберрискам, например, в виде тестирования, сертификации или страховки?
- Если вы не можете утвердительно ответить на один или более из вышеперечисленных вопросов, обратитесь к генеральному директору, директору по информационной безопасности, соответствующему персоналу организации и/или к внешним ресурсам, чтобы исправить проблему.

---

### НАДЗОР

- Убедитесь, что совет директоров осведомлен о своей конечной ответственности за киберриски и устойчивость организации.
  - При необходимости делегируйте надзор конкретному комитету совета директоров.
- Назначьте одного корпоративного директора, как правило, главного директора по информационной безопасности, ответственным за отчетность о способности организации управлять киберустойчивостью и развитием при достижении целей устойчивости к угрозам кибербезопасности.
  - Убедитесь, что этот сотрудник имеет регулярный доступ к совету директоров, обладает достаточными полномочиями, имеет в распоряжении соответствующий коллектив, опыт и ресурсы для выполнения этих обязанностей.
- Ежегодно определяйте допустимость рисков организации; обеспечьте согласованность с корпоративной стратегией и приемлемыми пределами рисков.
- Обеспечьте проведение ежегодного официального независимого анализа киберустойчивости организации.
- Обеспечьте интеграцию процедур обеспечения киберустойчивости и оценки рисков в общую бизнес-стратегию организации, управление рисками, планирование бюджета и распределение ресурсов.
- Обеспечьте контроль над созданием, внедрением, тестированием и постоянным совершенствованием планов по обеспечению киберустойчивости, обеспечением унификации во

всей организации, а также регулярностью представления отчетов перед советом директоров со стороны главного директора по информационной безопасности или других ответственных должностных лиц.

- Периодически проверяйте собственную эффективность и рассмотрите возможность получения независимых рекомендаций по непрерывному совершенствованию вашей системы.

---

## БУДЬТЕ В КУРСЕ

- При принятии в совет нового члена убедитесь, что этот сотрудник обладает применимыми и актуальными навыками и знаниями, позволяющими понимать связанные с киберугрозами риски.
- Регулярно консультируйтесь с руководством по текущим и будущим рискам в организации, соответствующим нормативным требованиям, а также отраслевым и социальным ориентирам для снижения приемлемых пределов риска. Запланируйте:
  - регулярные брифинги по обязанностям, соответствующим новым нормативным требованиям и законодательству;
  - совместное планирование советом директоров и исполнительным комитетом, а также визиты к коллегам и руководителям в области кибербезопасности;
  - брифинги по вопросам безопасности в среде кибербезопасности;
  - обмен информацией об управлении и отчетности на уровне совета.
- Информировать руководителей об их ответственности за предоставление количественно выраженной и доступно изложенной оценки киберрисков, угроз и событий в виде повестки дня во время заседаний совета директоров.
- Регулярно взаимодействуйте с руководителями и другими соответствующими сотрудниками и обсуждайте текущие системные проблемы, такие как уязвимость цепи поставок, общие зависимости, а также недостаток информации при обмене данными по вопросам управления киберрисками между советами директоров.

---

## СОЗДАНИЕ АТМОСФЕРЫ

- Убедитесь, что сотрудники на всех уровнях осознают важность своих обязанностей в обеспечении киберустойчивости организации.
- Контролируйте роль руководства в формировании и поддержании в организации культуры рисков. Регулярно оценивайте эффективность культуры рисков организации, принимая во внимание ее влияние на безопасность и надежность, а также при необходимости вносите необходимые корректировки.
- Четко объясните, что вы ожидаете от всех сотрудников добросовестного отношения и незамедлительного информирования обо всех случаях несоблюдения нормативных требований в организации или за ее пределами.

# КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

## КОНТРОЛЬНЫЙ СПИСОК ГЕНЕРАЛЬНОГО ДИРЕКТОРА: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

### УПРАВЛЕНИЕ

- Назначьте сотрудника на должность директора отдела информационной безопасности (CISO).
- Разработайте ориентированную на существующие риски политику кибербезопасности организации на основании международных, национальных и отраслевых стандартов и указаний, а также обеспечьте ее соблюдение.
- Определите роли и обязанности всех задействованных в обеспечении кибербезопасности сотрудников. Совместно с директором по информационной безопасности определите надлежащие роли в обеспечении кибербезопасности и права доступа для сотрудников всех уровней.
- Разработайте или определите четкие каналы связи между отдельными подразделениями или сотрудниками, работающими с различными аспектами кибербезопасности.
- Убедитесь, что директор по информационной безопасности имеет четкую прямую линию коммуникации для своевременного уведомления вас и совета директоров об угрозах.
- Регулярно приглашайте директора по информационной безопасности или другого технического специалиста для проведения брифинга перед высшим руководством.
- Убедитесь, что политики, стандарты и механизмы кибербезопасности унифицированы во всей организации.

### ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ ИМИ

- Совместно с директором по информационной безопасности или техническими специалистами проведите оценку рисков, предусматривающую:
  - описание активов организации и различных уровней их зависимостей от технологических ресурсов;
  - оценку зрелости организации и неотъемлемых рисков, связанных с зависимостями ее активов от технологических ресурсов;
  - определение желаемого состояния зрелости организации;
  - анализ приоритетных областей для обеспечения кибербезопасности в организации;
  - выявление несоответствий между текущим состоянием и желаемым целевым состоянием кибербезопасности;
  - реализацию планов для достижения и поддержания зрелости;
  - постоянную переоценку зрелости кибербезопасности организации, рисков и целей;
  - рассмотрение возможности принятия защитных мер, таких как приобретение киберстраховки.
- Обеспечьте проведение анализа и предоставление результатов ключевым заинтересованным сторонам и совету директоров.
- Запланируйте контроль всех мер, направленных на повышение осведомленности в сфере кибербезопасности, и отслеживание процесса их внедрения.

---

## ОРГАНИЗАЦИОННАЯ КУЛЬТУРА

- Регулярно обсуждайте вопросы киберрисков и кибербезопасности на уровне руководства.
- Убедитесь, что обучение принципам кибербезопасности является частью процесса адаптации всех сотрудников, и все сотрудники подписывают документы, подтверждающие их согласие соблюдать политики кибербезопасности организации.
- Организуйте регулярные курсы обучения по вопросам кибербезопасности для всех сотрудников.
- Убедитесь, что вопросы кибербезопасности всегда учитываются при оценке организацией потенциальных поставщиков и передаче данных третьим сторонам.
- Ежегодно пересматривайте политики кибербезопасности организации.
- Поощряйте добровольный обмен информацией об угрозах кибербезопасности и инцидентах между техническими специалистами.

# 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).



## КОНСУЛЬТИРОВАНИЕ КЛИЕНТОВ И СОТРУДНИКОВ ПО ВОПРОСАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Предоставьте сотрудникам и клиентам следующие личные рекомендации, которые помогут обеспечить защиту их данных:
  - [Используйте надежные пароли](#) на всех личных и профессиональных устройствах и рассмотрите возможность использования диспетчера паролей.
  - Регулярно [обновляйте](#) операционные системы, другое ПО и приложения на своих компьютерах и мобильных устройствах.
  - [Установите](#) антивирусное, антивредоносное ПО и защиту от программ-вымогателей для предотвращения, обнаружения и удаления вредоносных программ.
  - Используйте брандмауэр для предотвращения несанкционированного доступа к компьютеру.
  - Используйте продукты безопасности только от надежных компаний. Ознакомьтесь с отзывами о компьютерах и потребительскими изданиями, а также рассмотрите возможность консультации с производителем вашего компьютера или операционной системы.
  - Соблюдайте осторожность при работе с конфиденциальной информацией. Не отправляйте пароли от банковского счета или другие конфиденциальные данные финансового счета по незашифрованной электронной почте.
  - Соблюдайте осторожность в отношении того, где и как вы [подключаетесь к Интернету](#) для связи с банком или другого обмена конфиденциальной личной информацией.
  - Не открывайте вложения из электронных писем сразу после получения и не переходите по ссылкам в незапрошенных или подозрительных электронных письмах. Остановитесь. Подумайте. Нажмите на кнопку.
  - С подозрением относитесь к ситуациям, когда кто-то неожиданно обращается к вам через Интернет или по телефону и запрашивает личную информацию. Даже при общении с известными адресатами постарайтесь свести к минимуму обмен личной информацией по электронной почте.
  - Помните, что ни одно финансовое учреждение не будет отправлять электронные письма или звонить и запрашивать конфиденциальную информацию, которая у них уже имеется.
  - Предполагайте, что запрос на получение информации из банка, где вы никогда не открывали счет, является мошенничеством.
  - [Перед предоставлением](#) личной информации проверяйте достоверность подозрительного электронного письма или всплывающего окна. Обратите особое внимание на адрес электронной почты.

---

## УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ

- [Требуйте, чтобы для входа в ваши сервисы клиенты использовали надежные идентификаторы пользователей и пароли](#). Посоветуйте им не использовать пароль, который уже используется для других учетных записей.
- Для проверки реальных клиентов и снижения возможности мошенничества используйте мгновенную верификацию, проверку в реальном времени, пробную проверку вклада, проверку личности и/или ответы на личные вопросы.
- Предлагайте, а лучше — требуйте от клиентов прохождения двухфакторной аутентификации при входе в ваши сервисы.
- Регулярно проверяйте учетные записи пользователей на наличие признаков мошенничества.

---

## ЗАЩИТА ДАННЫХ

- Подумайте о том, какие данные клиентов организация должна собирать для предоставления своих услуг, и соблюдайте осторожность при сборе дополнительных данных клиентов.
- Разработайте и распространите политики хранения данных. Ликвидируйте данные клиентов, которые больше не будут использоваться.
- Обеспечьте шифрование передаваемых и неиспользуемых данных клиентов.
- Внедрите политики безопасности данных, чтобы четко обозначить разрешенные и запрещенные методы передачи данных и укажите допустимые процедуры для всех сотрудников при работе с данными клиентов. Убедитесь, что эти политики задокументированы, доведены до сведения всех сотрудников и периодически пересматриваются и обновляются.

---

## ЗАЩИТА ОБЩЕДОСТУПНЫХ ВЕБ-ПРИЛОЖЕНИЙ

- Обеспечьте внедрение протокола HTTPS в общедоступных веб-приложениях организации и перенаправляйте весь HTTP-трафик по протоколу HTTPS.
- Используйте политику безопасности контента на ваших веб-сайтах.
- Активируйте закрепление публичного ключа на ваших веб-сайтах.
- Убедитесь, что в общедоступных веб-приложениях не используются файлы «cookie» для хранения особо важной или критичной информации о клиентах (например, паролей) и что эти файлы имеют даты истечения срока действия (лучше раньше, чем позже).
- Рассмотрите возможность шифрования информации, хранящейся в используемых файлах «cookie».
- Рассмотрите возможность найма службы проверки на проникновение для оценки безопасности общедоступных веб-приложений не реже одного раза в год.

---

## ОБУЧЕНИЕ СОТРУДНИКОВ

- Обучайте своих сотрудников подотчетности и стратегиям минимизации человеческих ошибок, которые могут привести к раскрытию данных клиентов. Посоветуйте им:
  - свести к минимуму доступ к данным клиентов и их передачу, получая его только для выполнения своих должностных обязанностей;
  - придерживаться строгих методов обеспечения безопасности на всех устройствах и учетных записях, которые работают с данными клиентов, посредством использования надежных паролей, двухфакторной аутентификации, обновления ПО, и воздерживаться от перехода по подозрительным ссылкам;

- сообщать о любых потенциальных внутренних или внешних инцидентах в сфере безопасности, угрозах или неправильном обращении с данными клиентов техническим специалистам организации и/или высшему руководству.
- Убедитесь, что ваши сотрудники ознакомились с документами и подписали их, подтвердив согласие с политиками безопасности и защиты данных организации.

---

## УВЕДОМЛЕНИЕ КЛИЕНТОВ

- Обеспечьте понимание нормативных требований организации в отношении нарушений безопасности данных клиентов, чтобы гарантировать готовность к их соблюдению в случае подобных инцидентов.
- Когда ваша организация узнает о несанкционированном доступе к конфиденциальной информации клиентов, необходимо срочно провести расследование и определить вероятность того, что информация была или будет незаконно использоваться. Используйте передовые способы уведомления и незамедлительно сообщите пострадавшим клиентам следующие данные:
  - Общее описание происшествия и информацию, к которой был получен несанкционированный доступ.
  - Номер телефона для получения дополнительной информации и помощи.
  - Напоминание «сохранять бдительность» в течение следующих 12–24 месяцев.
  - Рекомендация о необходимости незамедлительного информирования о подозрениях в краже персональных данных.
  - Общее описание мер, предпринятых финансовым учреждением для защиты информации от дальнейшего несанкционированного доступа или использования.
  - Контактная информация бюро кредитных историй.
  - Любая другая информация, которая требуется в соответствии с соблюдаемыми организацией нормативными требованиями.

# КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

## ЗАЩИТА ОТНОШЕНИЙ С ТРЕТЬИМИ ЛИЦАМИ

---

### РЕКОМЕНДАЦИИ ПО ВЫБОРУ ПОСТАВЩИКОВ С УЧЕТОМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

При оценке потенциального поставщика вы должны рассмотреть следующие вопросы:

- Как они обслуживают клиентов, подобных вашей организации?
- Документировали ли они их соответствие установленным стандартам кибербезопасности, например, модели Национального института по стандартизации и технологии (NIST) или стандарту ISO 27001, а также могут ли они предоставить отчет SOC2?
- Какие из ваших данных и/или активов необходимы им для предоставления своих услуг?
- Как они планируют обеспечить защиту активов и данных вашей организации, находящихся в их распоряжении?
- Как они управляют собственными киберрисками, и могут ли они предоставить информацию по обеспечению безопасности цепи поставок?
- Каков их план аварийного восстановления и обеспечения непрерывности бизнеса в случае возникновения инцидента, затрагивающего активы и/или данные вашей организации?
- Как они будут информировать вашу организацию о тенденциях, угрозах и изменениях в своей организации?

---

### ВЫЯВЛЕНИЕ РИСКОВ В ОТНОШЕНИИ ТРЕТЬИХ ЛИЦ

Оцените киберриски в отношении сторонней организации, выполнив следующие шаги:

- Составьте и постоянно обновляйте список всех отношений с поставщиками, а также предоставляемых каждому из них активов и данных.
- Проведите анализ данных, к которым каждый поставщик или третье лицо имеет доступ, следуя принципу предоставления «наименьших привилегий».
- Оцените уровень риска отношений с поставщиками и сторонними организациями (низкий, средний, высокий), исходя из последствий получения несанкционированного доступа к их системам, для вашей организации.
- Начиная с поставщиков с самым высоким уровнем риска, оцените возможности обеспечения и соблюдения стандартов кибербезопасности каждого поставщика.
- Разработайте план регулярной оценки безопасности, в том числе оценки на рабочих объектах поставщиков с наивысшим уровнем риска и/или с большим доступом к данным клиентов.

---

### УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТРЕТЬИХ ЛИЦ

- Проведите тщательную комплексную проверку. Устанавливайте требования к уровню кибербезопасности для поставщиков в отношении всех предложений, контрактов, непрерывности бизнеса, процедур реагирования на инциденты и соглашений об уровне обслуживания. Согласуйте обязанности и обязательства в случае кибератак.
- Узнайте о методах обеспечения кибербезопасности финансовых организаций и других организаций, с которыми вы взаимодействуете или обмениваетесь данными, с учетом того, что ваши поставщики и сторонние организации должны соблюдать требования кибербезопасности, соблюдаемые вашей организацией.

- Используйте установленные и согласованные меры для осуществления контроля соблюдения стандартов кибербезопасности вашими поставщиками.
- Проверьте, предлагают ли ваши поставщики, обрабатывающие конфиденциальные данные, двухфакторную аутентификацию, шифрование и другие меры безопасности для всех используемых ими учетных записей.
- Убедитесь, что все устанавливаемое вами программное и аппаратное обеспечение оснащено системами безопасности для защиты процессов загрузки с помощью кодов аутентификации и отклонения загрузки в тех случаях, когда коды не распознаются.
- Если вы столкнулись с продукцией поставщика, которая является поддельной или не соответствует спецификациям, организуйте работу по решению вопроса или, если это невозможно, разработайте стратегию выхода.
- Проводите ежегодную оценку контрактов с поставщиками и убедитесь, что они продолжают соответствовать вашим стратегическим указаниям и требованиям в отношении безопасности данных. Включите в контракт положения о возврате ваших активов или данных после прекращения его действия, убедитесь, что активы или данные полностью удалены на стороне поставщика, и больше не предоставляйте ему доступ к вашим системам или серверам.

---

## ОБМЕН ИНФОРМАЦИЕЙ

- Убедитесь, что у вас есть четкие каналы связи и контакты для обмена сведениями о проблемах безопасности с поставщиками и партнерами вашей организации.
- Своевременно предоставляйте достоверную и актуальную информацию о кибербезопасности внутренним и внешним заинтересованным сторонам (в том числе организациям и государственным органам внутри и за пределами финансового сектора).
- Следите за актуальными обновлениями и новостями о том, с какими ситуациями сталкиваются другие организации, работающие со сторонними поставщиками, в отношении угроз, уязвимостей, инцидентов и решений проблем безопасности. Для этого вступайте в такие организации, как FS-ISAC, и изучайте прочие источники информации об угрозах.

# КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

## КОНТРОЛЬНЫЙ СПИСОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

### ПОДГОТОВКА

- Совместно с высшим руководством вашей организации и другими соответствующими сотрудниками разработайте план реагирования на инциденты и план обеспечения непрерывности бизнеса, исходя из наиболее актуальных рисков, выявленных в ходе оценки киберрисков организации.
- Разработайте сценарии угроз для инцидентов, связанных с наиболее приоритетными киберрисками организации. Сосредоточьтесь на наращивании потенциала для реагирования на эти сценарии.
- Определите, составьте и представьте в вашей организации список контактных лиц для реагирования на инциденты.
- Найдите и запишите контактные данные соответствующих местных и федеральных правоохранительных органов и должностных лиц.
- Установите положения, определяющие, о каких типах инцидентов необходимо сообщать, когда и кому.
- Определите и представьте в письменном виде указания, определяющие, как быстро персонал должен реагировать на инциденты и какие действия должны быть выполнены на основе соответствующих факторов, таких как функциональное и информационное воздействие инцидента, а также вероятной возможности восстановления после него.
- Сообщите всем сотрудникам, чтобы в случае инцидента они связывались с вашей технической командой. Обычно это ИТ-персонал и/или директор по информационной безопасности / директор по ИТ / другой подобный менеджер.
- Выполните развертывание решений для мониторинга действий сотрудников и выявления угроз и инцидентов.
- Включите планы по обеспечению непрерывности бизнеса для координации работы организации с поставщиками и основными клиентами во время чрезвычайной ситуации, в том числе при необходимости осуществления руководства или проведения альтернативных бизнес-операций.
- Включите определенные в письменном виде процедуры отключения и перезапуска системы в чрезвычайной ситуации.
- Обеспечьте разработку и тестирование методов извлечения и восстановления резервных данных. Периодически проверяйте резервные данные на предмет их целостности.
- Заключите соглашения и процедуры ведения коммерческой деятельности в альтернативном учреждении/центре.
- Обеспечьте работу четкого канала распространения для всех клиентов.
- Обеспечьте разработку и тестирование методов извлечения и восстановления резервных данных. Периодически проверяйте резервные данные на предмет их целостности.
- Заключите соглашения и процедуры ведения коммерческой деятельности в альтернативном учреждении/центре.
- Обеспечьте работу четкого канала распространения для всех клиентов.

---

## ОБУЧЕНИЕ

- Организуйте небольшие теоретические занятия со всеми сотрудниками или представителями персонала всех уровней, в том числе с руководителями организации, специалистами по связям с общественностью, сотрудниками юридического отдела и отдела нормативно-правового соответствия.
- Определите или лучше примите участие в отраслевых теоретических занятиях, связанных с деятельностью вашей организации.
- Разработайте процедуру проверки того, что сделанные в ходе занятий выводы включены в стратегию обеспечения кибербезопасности компании.

---

## РЕАГИРОВАНИЕ

- Внедрите действия плана реагирования на инциденты, чтобы свести к минимуму последствия для коммерческой деятельности.
- Определите поврежденные или находящиеся под угрозой системы и оцените повреждения.
- Для уменьшения ущерба выполните удаление (отключение) поврежденных активов.
- Начните запись всей информации сразу же после того, как команда выразит подозрения по поводу возможного инцидента. Попытайтесь сохранить доказательства инцидента при отключении/разделении поврежденных идентифицируемых активов, например, соберите данные о конфигурации системы, сети и журналов обнаружения вторжений из поврежденных активов.
- Уведомите соответствующие внутренние стороны, сторонних поставщиков и органы власти и при необходимости запросите поддержку.
- Иницируйте меры по уведомлению клиентов и оказанию помощи в соответствии с законами, нормативно-правовыми актами и межведомственным руководством.
- Используйте такие платформы обмена угрозами, как FS-ISAC или MISP для уведомления об угрозах других организаций из вашей отрасли.
- Задokumentируйте все предпринятые во время инцидента шаги для последующего анализа.

---

## ВОССТАНОВЛЕНИЕ

- По возможности восстановите активы с использованием периодических «точек восстановления» и используйте резервные данные для восстановления систем до последнего известного «исправного» состояния.
- Обеспечьте создание обновленных «чистых» резервных копий из восстановленных активов и убедитесь, что все резервные копии критически важных активов хранятся в физически защищенном месте.
- Выполните тестирование и убедитесь, что инфицированные системы полностью восстановлены. Убедитесь, что затронутые системы нормально функционируют.

---

## АНАЛИЗ

- Обсудите «сделанные выводы» после инцидента. Организуйте встречу с руководящим составом, доверенными советниками и поставщиками услуг поддержки аппаратного обеспечения для проведения анализа возможных уязвимостей или выработки рекомендаций по внедрению новых мер.
- По возможности определите уязвимости (будь то программное обеспечение, оборудование, бизнес-операции или поведение персонала), которые привели к инциденту и разработайте план по их устранению.
- Убедитесь, что затронутые системы нормально функционируют.

- Разработайте план мониторинга для выявления аналогичных или потенциально возможных инцидентов, связанных с выявленными проблемами.
- Поделитесь сделанными выводами и информацией об инциденте на платформах обмена угрозами, таких как FS-ISAC.
- Включите сделанные выводы в протоколы реагирования на произошедшие в организации инциденты.