ОПРОСНЫЙ ЛИСТ ПО АУДИТУ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ISO 27001

Наименование организации	
Контактное лицо	
Телефон	
Email	
Дата заполнения	

1. Цель проведения

☐ Оценка действующей системы информационной безопасности
☐ Подготовка к проверке регулятора
☐ Требования партнеров
☐ Другое

Указать

2. Существует в Вашей организации специализированное подразделение по информационной безопасности?

☐ Да ☐ Нет

Если да, то укажите, сколько человек в данном подразделении

Указать

3. Внедрена ли в Вашей организации система управления информационной безопасностью (СУИБ)?

☐ Да ☐ Нет

Если да, то опишите область действия системы управления информационной безопасностью

Указать

4. Какие из перечисленные ниже направления включены в зону ответственности подразделения информационной безопасности в Вашей организации?

☐ Делопроизводство
☐ Защита персональных данных
☐ Обеспечение непрерывности бизнеса/ восстановления деятельности после сбоев
☐ Охрана интеллектуальной собственности/коммерческой тайны
☐ Разработка приложений/систем
☐ Расследование мошеннических действий
☐ Реализация проектов и программ
☐ Управление активами
☐ Соблюдение нормативных требований в отношении ИТ (например, PCI DSS, ФЗ №152, ISO 27001, и т. д.)
☐ Управление рисками, связанными с отношениями с поставщиками
☐ Физическая безопасность
☐ Управление ИТ рисками

5. Укажите типы систем и количество пользователей

Тип системы	Количество пользователей «удаленные»	Количество пользователей «офисные»

6. Имеются ли процессы, переданные на аутсорсинг?

☐ Да ☐ Нет

Если да, то укажите какие

Указать

7. Перечень программно–технических средств

Укажите перечень программно–технических средств, включенных в область действия системы управления информационной безопасности

Указать

numbers of servers and desktops, types of networks, application development, access controls, use of encryption etc.

8. Утверждена ли в Вашей организации стратегия информационной безопасности на ближайшие 1–3 года?

☐ Да ☐ Нет

9. Утверждена ли в Вашей организации политика информационной безопасности?

☐ Да ☐ Нет

10. Какие из перечисленных ниже документов имеются в Вашей организации

☐ Область действия системы управления информационной безопасностью
☐ Политика информационной безопасности
☐ Методология оценки рисков
☐ Методология обработки рисков
☐ Положение о применимости
☐ План устранения рисков
☐ Отчет об оценке рисков
☐ Процедура управления документами
☐ Процедура управления записями
☐ Порядок внутреннего аудита
☐ Порядок и устранение неисправностей систем

- ☐ Определение ролей и обязанностей безопасности
- ☐ Политика управления доступом
- ☐ Принципы разработки защищенной системы
- ☐ Процедура управления инцидентами
- ☐ Процедуры непрерывности бизнеса
- ☐ Политика использования собственных устройств (BYOD)
- ☐ Мобильное устройство и политика удаленного доступа
- ☐ Политика классификации информации
- ☐ Парольная политика
- ☐ Политика уничтожения и утилизации
- ☐ Процедуры для работы в контролируемых зонах
- ☐ Политика чистого экрана и рабочего стола
- ☐ Политика управления изменениями
- ☐ Политика резервного копирования
- ☐ Политика передачи информации
- ☐ План тестирования системы информационной безопасности
- ☐ Стратегия непрерывности бизнеса
- ☐ Юридические, регулирующие и договорные требования
- ☐ Записи о степени подготовки, навыках, опыте и квалификации персонала
- ☐ Программа внутреннего аудита
- ☐ Результаты внутренних аудитов
- ☐ Результаты анализа со стороны руководства
- ☐ Результаты корректирующих действий
- ☐ Журналы пользовательских действий, исключений и событий безопасности

11. Какие из перечисленных ниже документов имеются в Вашей организации

- ☐ Да, для всех критичных ресурсов
- ☐ Да, для некоторых критичных ресурсов, работа не завершена
- ☐ Нет, не проведена

12. Какие из перечисленных ниже документов имеются в Вашей организации

- ☐ Да, для всех критичных ресурсов
- ☐ Да, для некоторых критичных ресурсов, работа не завершена
- ☐ Нет, не проведена

13. Какие из следующих видов тестирования на проникновение проводились в Вашей компании за последние 12 месяцев?

- ☐ Проведение анализа исходных кодов приложений
- ☐ Тестирование возможности внешнего проникновения из сети
- ☐ Тестирование защищенности внутренней инфраструктуры организации (операционных систем, баз данных, сетей)
- ☐ Анализ защищенности беспроводных сетей
- ☐ Тестирование защищенности средств предоставления удаленного доступа (модемные пулы, VPN)
- ☐ Проведение тестирования сотрудников организации с применением методов социальной инженерии
- ☐ Тестирование физического периметра путем физического проникновения в защищенные помещения и здания
- ☐ Тестирование защищенности систем IP-телефонии
- ☐ Иное

Указать

14. Какие механизмы используются в Вашей организации для повышения эффективности управления процессом информационной безопасностью?

Указать

15. Какова значимость перечисленных ниже последствий потери или хищения информации Вашей организации?

Риски	Значимость
Ущерб для репутации и бренда	
Снижение доходов	
Потеря клиентов	
Утрата доверия со стороны заинтересованных лиц	
Судебные/юридические разбирательства	
Ухудшение отношений с сотрудниками	
Нормативно-правовые действия/санкции	
Потеря конкурентных преимуществ (например, из-за потери объекта интеллектуальной собственности	

шкала оценок от 1 до 5, где 1 – "Наименее значимо", 5 – "Наиболее значимо"

16. Какие меры приняты в Вашей организации для минимизации потенциальных рисков, возникающих в результате сокращения штата?

- ☐ Проведение Оценка и совершенствование средств контроля за изменениями в информационных системах
- ☐ Оценка и совершенствование средств управления доступом и учетными записями
- ☐ Внедрение программы предотвращения утечки данных
- ☐ Разработка программы сохранения знаний, обеспечивающей сохранение знаний в случае увольнения ключевых сотрудников
- ☐ Меры не принимались
- ☐ Неприменимо
- ☐ Иное

Указать

17. Какие из следующих видов тестирования на проникновение проводились в Вашей компании за последние 12 месяцев?

Вид тестирования	Уровень		
Требования доступности информации	☐ Высокий	☐ Средний	☐ Низкий
Требования непрерывности бизнеса	☐ Высокий	☐ Средний	☐ Низкий
Выполнение нормативных и законодательных требований	☐ Высокий	☐ Средний	☐ Низкий

18. Какие из перечисленных ниже механизмов управления доступом и учетными записями внедрены в Вашей организации?

☐ Автоматизация процесса предоставления доступа (запрос, согласование, предоставление)
☐ Единый вход в корпоративные информационные системы (Single sign-on)
☐ Управление ролями пользователей
☐ Управление правами пользователей
☐ Управление учетными записями пользователе
☐ Управление паролями пользователей
☐ Многофакторная аутентификация (E-token, SmartCard, …)
☐ Защищенное хранение паролей/управление привилегированным доступом
☐ Виртуальный каталог/централизованное хранилище учетных записей
☐ Внедрение средств управления учетными записями
☐ Аутсорсинг отдельных мероприятий в области безопасности
☐ Управление доступом к веб-приложениям
☐ Централизованное журналирование и мониторинг
☐ Инфраструктура открытых ключей (Public Key Infrastructure – PK)
☐ Контроль за доступом в сеть/построение сетей (NAC)

19. Какие из перечисленных ниже средств в Вашей организации используются для контроля за утечкой конфиденциальной информации?

☐ Внедрены средства мониторинга/фильтрации контента
☐ Используются средства аудита
☐ Внедрены средства анализа журнала событий
☐ Доступ к конфиденциальной информации ограничен определенными периодами времени
☐ Применяется блокировка/ограничение использования отдельных компонентов аппаратного обеспечения (портов USB/ FireWire)
☐ Запрещено использование устройств со встроенной камерой в зонах ограниченного доступа
☐ Разработана специальная политика в отношении классификации конфиденциальной информации и порядка работы с ней
☐ Внедрены дополнительные механизмы безопасности в целях защиты информации (напр., шифрование)
☐ Ограничено/запрещено использование систем мгновенного обмена сообщениями или электронной почты для передачи конфиденциальной информации
☐ Сформулированы конкретные требования к пересылке/удаленному доступу к конфиденциальной информации
☐ Иное

Указать

20. Каким образом Вы проверяете, обеспечивают ли Ваши партнеры, поставщики или подрядчики необходимый уровень защиты Вашей информации при ее обработке, передачи и хранении?

☐ Анализ результатов оценок и иных сертификаций, проводимых внешними поставщиками или подрядчиками (например, ISO/IEC 27001, BS 25999)
☐ Анализ результатов проведения независимых оценок партнеров, поставщиков или подрядчиков, проведенных внешними организациями (например, SSAE 16)
☐ Проведение оценки силами Вашего подразделения информационной безопасности или службы внутреннего аудита (напр., выезд на место, тестирование системы безопасности)
☐ Анализ или оценка не проводится
☐ Иное

Указать

21. Какие из перечисленных ниже механизмов управления доступом и учетными записями внедрены в Вашей организации?

☐ Мы внедрили специальные контрольные процедуры для защиты персональных данных
☐ Используются средства аудита
☐ Сформулированы конкретные требования к пересылке/удаленному доступу к конфиденциальной информации
☐ Мы провели инвентаризацию информационных активов, на которые распространяются требования по защите персональных данных
☐ Внедрены дополнительные механизмы безопасности в целях защиты информации (напр., шифрование)
☐ Мы внедрили процедуру реагирования и управления инцидентами, относящимися к защите персональных данных
☐ Мы включили требования по защите персональных данных в договоры с независимыми партнерами, поставщиками и подрядчиками
☐ Мы имеем четкое представление о законодательных и нормативных актах в области защиты персональных данных, которые могут оказать влияние на нашу организацию
☐ Мы провели оценку жизненного цикла персональных данных (сбор, использование, хранение, передача и уничтожение)
☐ Мы внедрили процесс мониторинга и сопровождения контрольных процедур, связанных с защитой персональных данных

22. Включены ли в договоры, заключаемые Вашей организацией с клиентами, партнерами или подрядчиками, конкретные требования по обеспечению информационной безопасности?

☐ Да, все договора включают в себя конкретные требования к обеспечению информационной безопасности
☐ Да, отдельные договора включают в себя конкретные требования к обеспечению информационной безопасности
☐ Нет, конкретные требования к обеспечению информационной безопасности не включаются в договора☐ Мы провели оценку жизненного цикла персональных данных (сбор, использование, хранение, передача и уничтожение)
☐ Мы внедрили процесс мониторинга и сопровождения контрольных процедур, связанных с защитой персональных данных

23. Какие из перечисленных пунктов входят в программу по обеспечению непрерывности бизнеса в Вашей организации?

☐ Установленные отношения с местными экстренными службами (пожарные, полиция, скорая медицинская помощь)
☐ Определение очередности восстановления критичных бизнес-процессов
☐ Согласованные полномочия и обязанности всех участников группы по восстановлению в условиях инцидента или кризисной ситуации
☐ Выявление и оценка основных угроз и рисков, влияющих на непрерывность деятельности
☐ Процедуры управления инцидентами или кризисной ситуацией (в том числе, порядок эскалации кризисной ситуации, а также внутренние и внешние коммуникации)
☐ План восстановления ИТ инфраструктуры после сбоев (IT DRP)
☐ Процедуры восстановления бизнес-процессов
☐ План тестирования системы обеспечения непрерывности бизнеса, включающий в себя обзор упражнений и тестов
☐ Стратегия по обеспечению непрерывности бизнеса, направленная на восстановление ИТ и телекоммуникаций, сопутствующей инфраструктуры, а также критичных бизнес-процессов в случае экстренной ситуации
☐ Планы повышения осведомленности и обучения персонала по вопросам обеспечения

непрерывности бизнеса

24. Каким образом в Вашей организации проходит оценка программы по обеспечению непрерывности деятельности?

- ☐ Установленные отношения с местными экстренными службами (пожарные, полиция, скорая медицинская помощь)
- ☐ Определение очередности восстановления критичных бизнес-процессов
- ☐ Согласованные полномочия и обязанности всех участников группы по восстановлению в условиях инцидента или кризисной ситуации
- ☐ Выявление и оценка основных угроз и рисков, влияющих на непрерывность деятельности
- ☐ Процедуры управления инцидентами или кризисной ситуацией (в том числе, порядок эскалации кризисной ситуации, а также внутренние и внешние коммуникации)
- ☐ План восстановления ИТ инфраструктуры после сбоев (IT DRP)
- ☐ Процедуры восстановления бизнес-процессов
- ☐ План тестирования системы обеспечения непрерывности бизнеса, включающий в себя обзор упражнений и тестов
- ☐ Стратегия по обеспечению непрерывности бизнеса, направленная на восстановление ИТ и телекоммуникаций, сопутствующей инфраструктуры, а также критичных бизнес-процессов в случае экстренной ситуации
- ☐ Планы повышения осведомленности и обучения персонала по вопросам обеспечения непрерывности бизнеса

25. Укажите, как в Вашей организации построено взаимодействие с ключевыми контрагентами в контексте обеспечения непрерывности деятельности?

Указать

26. Какие вопросы рассматриваются в программе повышения осведомленности по вопросам безопасности, принятой в Вашей организации?

- ☐ Повышение осведомленности по вопросам обеспечения информационной безопасности
- ☐ Проверка, согласование и соблюдение действующих политик и стандартов в области безопасности
- ☐ Оценка эффективности мероприятий по повышению осведомленности и улучшение существующей программы на основании результатов такой оценки
- ☐ Распространение наглядных и регулярных новостей/оповещений о существующих угрозах для Вашей организации
- ☐ Распространение информационных сводок по новым актуальным темам
- ☐ Проведение специальных мероприятий или тренингов в области безопасности для пользователей, входящих в группы высокого риска
- ☐ Иное

Указать

27. Какие из перечисленных ниже технологий Ваша организация использует?

- ☐ Радио частотные
- ☐ Беспроводная связь
- ☐ Виртуализация серверов VoIP Системы управления доступом и учетными записями
- ☐ Шифрование съемных носителей
- ☐ Шифрование электронной почты
- ☐ Шифрование данных на жестких дисках настольных компьютеров
- ☐ Облачные вычисления
- ☐ Многофакторная аутентификация (802.1x, токены)
- ☐ Программные средства корпоративного управления, управления рисками и соблюдения нормативных требований
- ☐ Средства мониторинга/фильтрации контента
- ☐ Средства предотвращения утечки данных
- ☐ Технические средства защиты авторских прав
- ☐ Шифрование данных на жестких дисках ноутбуков
- ☐ Использование биометрических средств
- ☐ Распределенные вычисления
- ☐ Совмещение физической и логической безопасности (например, объединение параметров физического и логического доступа)

28. Желаемый перечень работ по аудиту соответствия требованиям ISO 27001

- ☐ Обследование текущего состояния СУИБ
- ☐ Проектирование СУИБ
- ☐ Проведение оценки рисков ИБ
- ☐ Внедрение СУИБ

29. Желаемый перечень сопутствующих работ

- ☐ Проведение тестирования на проникновение и анализа защищенности
- ☐ Разработка модели угроз по новой методике ФСТЭК

30. Желаемый перечень иных работ

- ☐ Приведение в соответствие требованиям 716-П
- ☐ Аудит организации в направлении обработки/защиты персональных данных
- ☐ Независимая внешняя оценка SWIFT
- ☐ Аудит на соответствие требованиям 719-П, 757-П, 683-П, 802-П, иных источников требований ЦБ/Приведение в соответствие требованиям 719-П, 757-П, 683-П, 802-П, иных источников требований ЦБ
- ☐ Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580
- ☐ Анализ платежного ПО по ОУД4

31. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ

- ☐ Планируется ли поставка решений ИБ/ИТ?
- ☐ Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ?

Какие решения по ИБ/ИТ вами рассматриваются?

Указать

Благодарим за уделенное время!

Если вы затрудняетесь с заполнением, то мы готовы вам помочь.

Укажите удобную дату и время для встречи		
Дата		
Диапазон времени	*от*	*до*
Желательный способ связи	*Указать*	