ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Академия безопасности бизнеса

Барбашёв Сергей Анатольевич
тел. 509-3482, e-mail: abb@fapsi.net
http://abb.fapsi.net

ЭТАПЫ	1. АНАЛИЗ состава и содержания конфиденциальной информации
Какие вопросы надо решать?	Какие сведения следует охранять? Кого интересуют охраняемые сведения, когда? Почему они нуждаются в получении этих сведений?
Ответственные исполнители	Руководство организации, предприятия.
Какие мероприятия следует провести	Обеспечить изучение вопросов состояния секретности и защиты информации. Составить подробный обзор всех информационных потоков. Проверить обоснованность и необходимость информационных потоков.
Что особенно нужно учитывать?	Оценить необходимость накопленной информации.
Какие документы разрабатываются	Информационная модель организации предприятия.

ЭТАПЫ	2. АНАЛИЗ ценности информации
Какие вопросы надо решать?	Какие виды информации имеются? Какова ценность каждого вида информации? Какая защита необходима для информации?
Ответственные исполнители	Администрация
Какие мероприятия следует провести	Установить правовые и законодательные требования. Разработать принципы определения ценности информации. Определить ценность каждого вида информации.
Что особенно нужно учитывать?	Законодательную ответственность администрации за безопасность информации. Степень ущерба при раскрытии, потере, ошибках в информации.
Какие документы разрабатываются	Структура и принципы классификации информации. Законодательные требования, инструкции, нормы.

ЭТАПЫ	3. ОЦЕНКА уязвимости информации
Какие вопросы надо решать?	Какие каналы утечки информации имеются? Какова степень уязвимости каналов утечки? Насколько уменьшится уязвимость информации при использовании системы и средств защиты?
Ответственные исполнители	Специалисты отдела безопасности.
Какие мероприятия следует провести	Составить перечень каналов утечки информации. Составить перечень уязвимых помещений. Установить приоритеты информации, определить охраняемые сведения. Классифицировать информацию по приоритетам и ценности.
Что особенно нужно учитывать?	Распределение приоритетов информации, требующей защиты, путем определения относительной уязвимости и степени секретности.
Какие документы разрабатываются	Классификаторы информации и каналов утечки.

ЭТАПЫ	4. ИССЛЕДОВАНИЕ действующей системы защиты информации
Какие вопросы надо решать?	Какие меры безопасности используются? Каков уровень организации защиты информации? Какова стоимость доступных мер защиты информации? Какова эффективность действующей системы защиты информации?
Ответственные исполнители	Администрация, линейное руководство, отдел безопасности.
Какие мероприятия следует провести	Составить аналитический обзор действующей системы защиты информации. оценить затраты и степень риска при действующей системе защиты информации.
Что особенно нужно учитывать?	Усиление безопасности не остановит злоумышленника. Что новая технология может быть эффективнее по критерию эффективности/стоимости.
Какие документы разрабатываются	Аналитический обзор действующей СЗИ и ее безопасность.

ЭТАПЫ	5. ОЦЕНКА затрат на разработку новой системы защиты информации
Какие вопросы надо решать?	Какова стоимость новой системы защиты? Какой уровень организации новой системы? Какая стоимость доступна и какая велика? Какой выигрыш будет получен при новой системе?
Ответственные исполнители	Администрация, финансово-плановая служба.
Какие мероприятия следует провести	Разработать план реализации замысла на создание новой системы защиты информации. Изыскать необходимые ресурсы.
Что особенно нужно учитывать?	Установить требования по финансированию и его источники.
Какие документы разрабатываются	Средства СЗИ. Бюджет на разработки. Внедрение и сопровождение новой СЗИ.

ЭТАПЫ	6. ОРГАНИЗАЦИЯ мер защиты информации
Какие вопросы надо решать?	Какие проявляются новые функции? Какой потребуется новый персонал? Какая квалификация необходима для выполнения новых обязанностей?
Ответственные исполнители	Администрация, линейное руководство, отдел безопасности.
Какие мероприятия следует провести	Определить ответственность за безопасность информации в каждом подразделении. Подготовить инструкцию по организации защиты информации.
Что особенно нужно учитывать?	Важность организационных мер защиты информации.
Какие документы разрабатываются	Организационно-функциональная схема СЗИ. Порядок и правила работы в новых условиях.

ЭТАПЫ	7. ЗАКРЕПЛЕНИЕ персональной ответственности за защиту информации
Какие вопросы надо решать?	Какие конкретно сотрудники имеют доступ к охраняемым сведениям? Проверены ли эти сотрудники на благонадежность?
Ответственные исполнители	Линейное руководство, отдел безопасности.
Какие мероприятия следует провести	Проверить персонал, обрабатывающий секретную информацию. Подготовить перечни секретных сведений для всех сотрудников.
Что особенно нужно учитывать?	Необходимость регулярного контроля за работой системы защиты информации.
Какие документы разрабатываются	Профили секретности сотрудников и линейных подразделений.

ЭТАПЫ	8. РЕАЛИЗАЦИЯ технологии защиты информации
Какие вопросы надо решать?	Каков приоритет секретной информации изделий? Какие дополнительные ресурсы потребуются? Кто отвечает за согласование проекта СЗИ с партнерами? Замысел реализации проекта.
Ответственные исполнители	Административная группа реализации отдела проекта, отдел безопасности, линейное руководство.
Какие мероприятия следует провести	Разработать планы реализации проекта новой системы защиты информации. Определить контрольные сроки и позиции их выполнения.
Что особенно нужно учитывать?	Полноту реализации требований новой системы защиты информации.
Какие документы разрабатываются	Подробный бюджет проекта новой СЗИ.

ЭТАПЫ	9. СОЗДАНИЕ обстановки сознательного отношения к защите информации
Какие вопросы надо решать?	Ориентирована ли политика организации на защиту информации? Имеется ли программа подготовки и обучения сотрудников организации в новых условиях работать с СЗИ?
Ответственные исполнители	Линейное руководство, отдел безопасности, ответственные за безопасность информации.
Какие мероприятия следует провести	Разработать программы подготовки сотрудников. Оценить личные качеств сотрудников по обеспечению безопасности информации.
Что особенно нужно учитывать?	Необходимость комплексной защиты информации. Сознательное отношение к защите информации и бдительность всего персонала.
Какие документы разрабатываются	Руководство по защите конфиденциальной информации. Программа обучения сотрудников.

ЭТАПЫ	10. КОНТРОЛЬ И ПРИЕМ в эксплуатацию новой системы защиты
Какие вопросы надо решать?	Какой должен быть состав специальной группы приема системы? Имеются ли стандарты безопасности и секретности информации? Насколько эффективна новая система защиты информации? Какие улучшения можно произвести?
Ответственные исполнители	Группа ревизии, приема и контроля работы СЗИ.
Какие мероприятия следует провести	Утвердить состав группы ревизии. Рассмотреть законодательные требования. Переоценить уязвимость информации и степень риска. Оценить точность и полноту реализации проекта.
Что особенно нужно учитывать?	Оценить реальную эффективность новой системы защиты. Необходимость систематического контроля за работой СЗИ.
Какие документы разрабатываются	Отчет и рекомендации, выработанные группой ревизии.