ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Академия безопасности бизнеса

Барбашёв Сергей Анатольевич

тел. 509-3482, e-mail: <u>abb@fapsi.net</u>

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

Что особенно нужно

Какие документы

разрабатываются

провести

учитывать?

Обеспечить изучение вопросов состояния

Проверить обоснованность и необходимость

секретности и защиты информации.

Оценить необходимость накопленной

Информационная модель организации

Составить подробный обзор всех

информационных потоков.

информационных потоков.

информации.

предприятия.

ЭТАПЫ2. АНАЛИЗ ценности информацииКакие вопросы надо решать?Какие виды информации имеются? Какова
ценность каждого вида информации?
Какая защита необходима для информации?Ответственные...

Администрация

требования.

информации.

информации.

информации.

нормы.

Установить правовые и законодательные

Определить ценность каждого вида

Законодательную ответственность

ошибках в информации.

Разработать принципы определения ценности

администрации за безопасность информации.

Степень ущерба при раскрытии, потере,

Структура и принципы классификации

Законодательные требования, инструкции,

исполнители

провести

учитывать?

Какие мероприятия следует

Что особенно нужно

Какие документы

разрабатываются

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.
	Распределение приоритетов информации,

требующей защиты, путем определения

учитывать? относительной уязвимости и степени секретности.

Какие документы Классификаторы информации и каналов разрабатываются утечки.

Что особенно нужно

ЭТАПЫ	защиты информации
	Какие меры безопасности используются? Каков уровень организации защиты информации?
Какие вопросы надо решать?	Какова стоимость доступных мер защиты

безопасности.

злоумышленника.

безопасность.

Ответственные

Какие мероприятия следует

Что особенно нужно

Какие документы

разрабатываются

исполнители

провести

учитывать?

информации? Какова эффективность

системы защиты информации.

оценить затраты и степень риска при

Усиление безопасности не остановит

по критерию эффективности/стоимости.

действующей системы защиты информации?

Администрация, линейное руководство, отдел

Составить аналитический обзор действующей

действующей системе защиты информации.

Что новая технология может быть эффективнее

Аналитический обзор действующей СЗИ и ее

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.

Средства СЗИ.

Бюджет на разработки.

Внедрение и сопровождение новой СЗИ.

Какие документы

разрабатываются

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 конкретно сотрудники имеют доступ к охраняемым сведениям? Проверены ли эти сотрудники на благонадежность?
Ответственные исполнители	Линейное руководство, отдел безопасности.

подразделений.

Какие мероприятия следует

Что особенно нужно

Какие документы

разрабатываются

провести

учитывать?

Проверить персонал, обрабатывающий

секретных сведений для всех сотрудников.

Необходимость регулярного контроля за

работой системы защиты информации.

секретную информацию. Подготовить перечни

Профили секретности сотрудников и линейных

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.

руководство.

Ответственные

Какие мероприятия следует

Что особенно нужно

Какие документы

разрабатываются

исполнители

провести

учитывать?

Административная группа реализации отдела

Разработать планы реализации проекта новой

контрольные сроки и позиции их выполнения.

системы защиты информации. Определить

Полноту реализации требований новой

Подробный бюджет проекта новой СЗИ.

системы защиты информации.

проекта, отдел безопасности, линейное

ЭТАПЫ	9. СОЗДАНИЕ обстановки сознательного отношения к защите информации
	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.
	Разработать программы подготовки

информации.

информации.

информации.

сотрудников. Оценить личные качеств

Необходимость комплексной защиты

и бдительность всего персонала.

Программа обучения сотрудников.

сотрудников по обеспечению безопасности

Руководство по защите конфиденциальной

Сознательное отношение к защите информации

Какие мероприятия следует

Что особенно нужно

Какие документы

разрабатываются

провести

учитывать?

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	Отчет и рекомендации, выработанные группой

ревизии.

разрабатываются