Методологические основы обеспечения информационной безопасности объекта

1. Основные термины и определения из области информационной безопасности
2. Принципы построения системы информационной безопасности объекта
3. Требования к системе информационной безопасности объекта
4. Последовательность действий при разработке системы обеспечения информационной безопасности объекта

Под безопасностью информации будем понимать такое ее состояние, при котором исключается возможность **ознакомления** этой информацией, ее **изменения** или **уничтожения** лицами, не имеющими на это права, а также **утечки** за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.

Под защитой информации понимается совокупность мероприятий, направленных на обеспечение **конфиденциальности** и **целостности** обрабатываемой информации, а также **доступности** информации для пользователей.

Конфиденциальность – содержание критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций) в **секрете**.

Целостность - свойство, при выполнении которого информация сохраняет заранее определенные **вид и качество**.

Доступность - такое состояние информации, когда она **находится в виде и месте**, необходимом пользователю, и **в то время**, когда она ему необходима.

Цель защиты информации - **сведение к минимуму потерь в управлении** вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Принцип непрерывности совершенствования и развития системы информационной безопасности.

Суть принципа заключается в постоянном контроле функционирования системы, выявлении слабых мест, потенциально возможных каналов утечки информации и НСД, обновлении и дополнении механизмов защиты **в зависимости от изменения характера внутренних и внешних угроз**, обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты информации.

Обеспечение информационной безопасности не может быть одноразовым актом !!!.

Принцип комплексного использования

всего арсенала имеющихся средств защиты **во всех структурных элементах** производства и **на всех этапах технологического цикла** обработки информации.

Комплексный характер защиты информации проистекает, прежде всего, из характера действий злоумышленников, стремящихся любой совокупностью средств добыть важную для конкурентной борьбы информацию.

Оружие защиты должно быть адекватно оружию нападения !!!.

Наибольший эффект достигается в том случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм — **систему информационной безопасности.**

Только в этом случае появляются **системные свойства** не присущие ни одному из отдельных элементов системы защиты, а также возможность **управлять системой**, **перераспределять ее ресурсы и применять современные методы повышения эффективности ее функционирования**.

Система информационной безопасности - организованная совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа к ней.

Важнейшими условиями обеспечения безопасности являются:

- **законность**
- **разумная достаточность**
- **соблюдение баланса интересов личности и предприятия**
- **высокий профессионализм службы информационной безопасности,**
- **подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности**
- **взаимная ответственность персонала и руководства**
- **взаимодействие с государственными правоохранительными органами.**

Без соблюдения этих условий никакая система информационной безопасности не может обеспечить требуемого уровня защиты !!!

Требования к системе защиты информации:

- **централизованность**; процесс управления *всегда централизован*, в то время как *структура системы*, реализующей процесс, должна *соответствовать структуре защищаемого объекта*;
- **плановость**; планирование осуществляется *для организации взаимодействия* подразделений объекта *в интересах реализации принятой политики безопасности*; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;
- **конкретность и целенаправленность**; защите подлежат абсолютно конкретные информационные ресурсы, могущие представлять интерес для конкурентов;
- **активность**; защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности *средств прогнозирования, экспертных систем и других инструментариев*, позволяющих реализовать наряду с принципом *"обнаружить и устранить"* принцип ***"предвидеть и предотвратить"***;
- **надежность и универсальность, охват всего технологического комплекса информационной деятельности объекта**; методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;
- **нестандартность** (по сравнению с другими организациями), разнообразие средств защиты;
- **открытость** для изменения и дополнения мер обеспечения безопасности информации;
- **экономическая эффективность**; затраты на систему защиты не должны превышать размеры возможного ущерба.

Устоявшиеся рекомендации,

которые будут не бесполезны создателям систем информационной безопасности:

- **простота технического обслуживания и “прозрачность”** средства защиты *для пользователей*;

- **минимальный набор привилегий**, необходимых для работы каждого пользователя ;

- **возможность отключения защиты в особых случаях**, когда механизмы защиты реально мешают выполнению работ;

- **независимость системы защиты от субъектов защиты**;

- разработчики системы защиты информации должны предполагать, что **пользователи имеют наихудшие намерения** (враждебность окружения), что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты;

- **отсутствие** на предприятии **излишней информации** о существовании механизмов защиты.

Цели и задачи, принципы построения и требования к системе защиты информации

Облик будущей системы информационной безопасности

ПОСЛЕДОВАТЕЛЬНОСТЬ РАЗРАБОТКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные этапы создания системы информационной безопасности	Результаты действий на каждом этапе создания системы информационной безопасности
1. Выявление информации, представляющей интеллектуальную собственность организации.	Список сведений, составляющих коммерческую тайну, и организаций (частных лиц), которых эти сведения могут интересовать
2.Определение границы управляемой информационной безопасностью.	Топологическая модель объекта с выявлением возможных точек нападения
3. Анализ уязвимости: - каналы утечки и НСД, - вероятность реализации угроз (установление информационного контакта), - модель действий нарушителя, - оценка ущерба (потерь).	Сценарий осуществления противоправных действий Ранжирование угроз п о вероятности их осуществления и возможному ущербу Принятие стратегии управления рисками
4. Выбор контрмер, обеспечивающих информационную безопасность.	Правовые, организационные и инженерно-технические мероприятия. Определение политики безопасности
5. Проверка системы защиты информации: - оценка эффективности вариантов построения, - тестирование системы.	Формирование системы информационной безопасности на основе результатов оценки эффективности и тестирования
6. Составление плана защиты.	Пакет документов по построению системы информационной безопасности и реализации политики безопасности
7. Реализация плана защиты информации.	Монтаж и настройка оборудования, управление системой защиты

ЭТАПЫ	1. АНАЛИЗ состава и содержания конфиденциальной информации	2. АНАЛИЗ ценности информации	3. ОЦЕНКА уязвимости информации	4. ИССЛЕДОВАНИЕ действующей системы защиты информации
Какие вопросы ешать? надо р	Какие сведения следует охранять? Кого интересуют охраняемые сведения, когда? Почему они нуждаются в получении этих сведений?	Какие виды информации имеются и какова ценность каждого из них? Какая защита необходима для информации?	Какие каналы утечки информации имеются и какова степень их уязвимости? Насколько уменьшится уязвимость информации при использовании системы и средств защиты?	Какие меры безопасности пользуются и какова эффективность действующей системы защиты? Какова стоимость доступных мер защиты информации?
Ответственные исполнители	Руководство организации, предприятия	Администрация	Специалисты отдела безопасности	Администрация, линейное руководство, отдел безопасности
Какие мероприятия следует провести	Обеспечить изучение вопросов состояния секретности и защиты информации Составить подробный обзор всех информационных потоков Проверить обоснованность и необходимость информационных потоков	Установить правовые и законодательные требования Разработать принципы определения ценности информации Определить ценность каждого вида информации	Составить перечень каналов утечки информации. Составить перечень уязвимых помещений. Установить приоритеты информации, определить охраняемые сведения. Классифицировать информацию по приоритетам и ценности	Составить аналитический обзор действующей системы защиты информации. О ценить затраты и степень риска при действующей системе защиты информации
Что особенно нужно учитывать?	Оценить необходимость накопленной информации	Законодательную ответственность администрации за безопасность информации Степень ущерба при раскрытии, потере, ошибках в информации	Распределение приоритетов информации, требующей защиты, путем определения относительной уязвимости и степени секретности	Усиление безопасности не остановит злоумышленника. Новая технология может быть эффективнее по критерию эффективность / стоимость
Какие документы разрабатываются	Информационная модель организации предприятия	Наличие нормативных документов. Структура и принципы классификации информации. Законодательные требования, инструкции, нормы	Классификаторы информации и каналов утечки	Аналитический обзор действующей СЗИ и ее безопасность

5. ОЦЕНКА затрат на разработку новой системы защиты информации	6. ОРГАНИЗАЦИЯ мер защиты информации	7. ЗАКРЕПЛЕНИЕ ответственности за защиту информации	8. РЕАЛИЗАЦИЯ технологии защиты информации	9. СОЗДАНИЕ обстановки сознательного отношения к защите информации	10. КОНТРОЛЬ И ПРИЕМ в эксплуатацию новой системы защиты
Какой уровень организации новой системы? Какой выигрыш будет получен при новой системе? Какова стоимость новой системы защиты и доступна ли она?	Какие появляются новые функции? Какой потребуется новый персонал и какая квалификация необходима для выполнения новых обязанностей?	Какие конкретно сотрудники имеют доступ к охраняемым сведениям? Проверены ли эти сотрудники на благонадежность?	Каков приоритет секретной информации? Какие дополнительные ресурсы потребуются? Кто отвечает за согласование проекта СЗИ с партнерами? Замысел реализации проекта	Ориентирована ли политика организации на защиту информации? Имеется ли программа подготовки и обучения сотрудников организации в новых условиях работать с СЗИ?	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?
Администрация, финансово-плановая служба	Администрация, линейное руководство, отдел безопасности	Линейное руководство, отдел безопасности	Административная группа реализации отдела проекта, отдел безопасности, линейное руководство	Линейное руководство, отдел безопасности, ответственные за безопасность информации	Группа ревизии, приема и контроля работы СЗИ
Разработать план реализации замысла на создание новой системы защиты информации Изыскать необходимые ресурсы	Определить ответственность за безопасность информации в каждом подразделении. Подготовить инструкцию по организации защиты информации	Проверить персонал, обрабатывающий секретную информацию, Подготовить перечни секретных сведений для всех сотрудников	Разработать планы реализации проекта новой системы защиты информации. Определить контрольные сроки и позиции их выполнения	Разработать программы подготовки сотрудников. Оценить личные качеств сотрудников по обеспечению безопасности информации	Утвердить состав группы ревизии. Рассмотреть законодательные требования. Переоценить уязвимость информации и степень риска. Оценить точность и полноту реализации проекта
Установить требования по финансированию и его источники	Важность организационных мер защиты информации	Необходимость регулярного контроля за работой системы защиты информации	Полноту реализации требований новой системы защиты информации	Необходимость комплексной защиты информации Сознательное отношение к защите информации и бдительность всего персонала	Оценить реальную эффективность новой системы защиты Необходимость систематического контроля за работой СЗИ
Средства СЗИ Бюджет на разработки Внедрение и сопровождение новой СЗИ	Организационно-функциональная схема СЗИ Порядок и правила работы в новых условиях	Профили секретности сотрудников и линейных подразделений	Подробный бюджет проекта новой СЗИ	Руководство по защите конфиденциальной информации Программа обучения сотрудников	Отчет и рекомендации, выработанные группой ревизии