Колледж связи 54

Подразделения ТЗИ
и их основные задачи

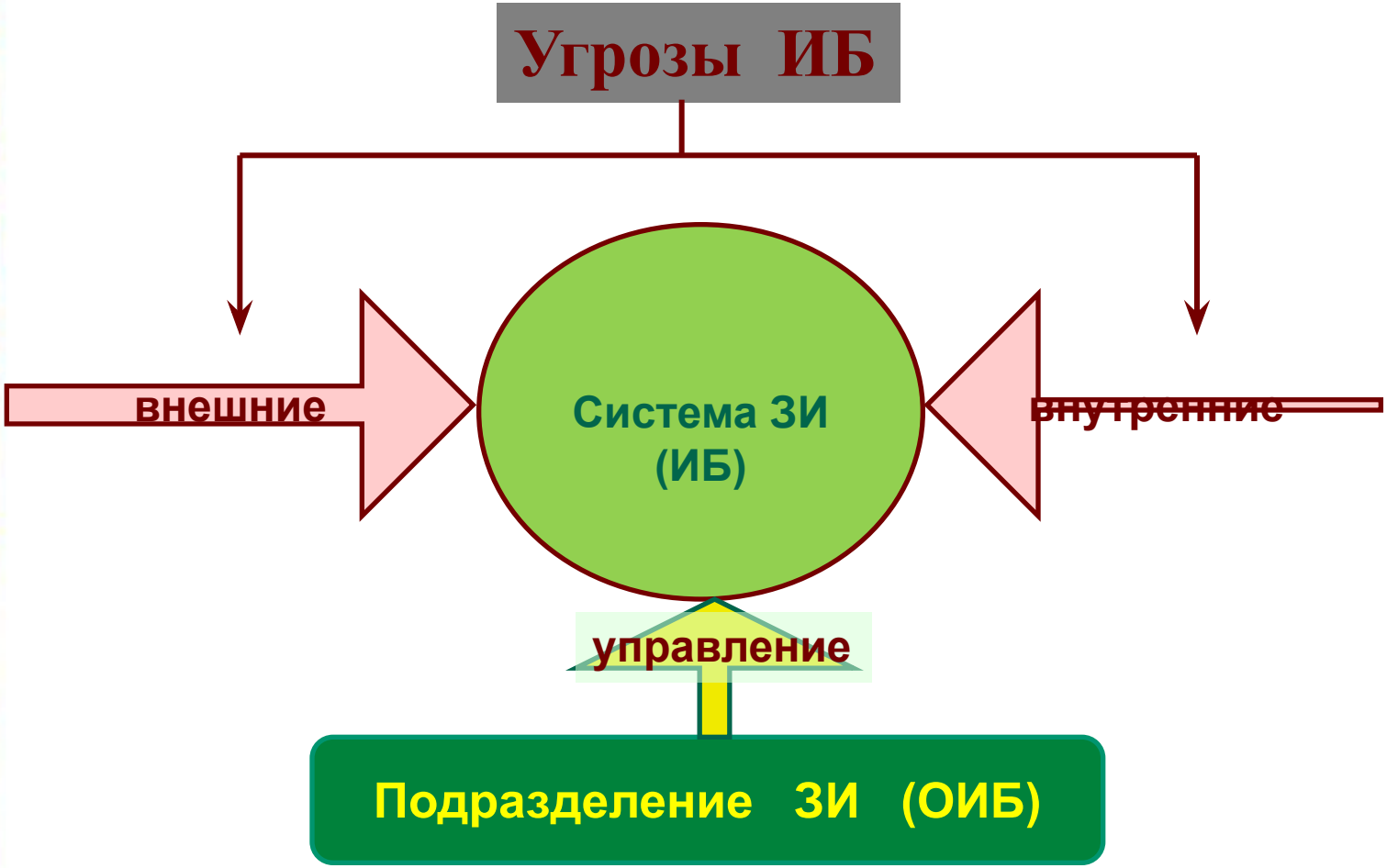
Какова цель подразделения защиты информации?

Предотвращение (минимизация) ущерба, наносимого информационным ресурсам организации (предприятия, органа власти …..) за счет нарушения свойств безопасности информации.

Ущерб может быть прямым, косвенным, материальным, моральным, репутационным, …

Цель и задачи подразделения защиты информации

Цель – минимизация рисков ИБ



Задача – управление СИБ

Условия деятельности подразделения ЗИ (ОИБ)

- Наличие полной и непротиворечивой нормативно-правовой базы по вопросам ОИБ;
- Наличие ресурсов (финансовых, технических, человеческих, организационных, …);
- Определение целей, задач и функций подразделения ЗИ;
- Наличие системы (средств) управления ЗИ;

Факторы, определяющие структуру подразделения ЗИ (ОИБ)

1. Вид деятельности предприятия;

2. Масштаб и структура предприятия;

3. Наличие внешних связей;

4. Структура информационных систем и информационных потоков (бизнес-процессов);

5. Степень важности обрабатываемой информации;

6. Угрозы ИБ;

7. Располагаемые ресурсы.

8. Функции подразделения ЗИ.

Идеальных структур «на все случаи жизни» не бывает!

Функции (задачи) службы информационной безопасности (службы защиты информации)

Анализ и выявление угроз защищаемой информации, причин и условий их возникновения и реализации.

Выявление и максимальное устранение (минимизация) потенциально возможных каналов утечки и несанкционированного доступа к информации.

Внедрение механизмов нейтрализации угроз (применение юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности информации).

Организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

- Информационно-аналитическая деятельность
- Защита информации от УТК
- Защита информации от НСД
- Организационные мероприятия по ЗИ
- Работа с документами конф. характера

Варианты функционирования подразделения (службы) ИБ

Вариант 1, 2.
Один или группа специалистов по ИБ внутри ИТ- департамента

Преимущества:

Вариант легко реализуем, поскольку не требует создания обособленной структуры.
Возможность работы напрямую во внутренних или внешних ИТ-проектах , что способствует внедрению требований по ИБ на этапе реализации проектов (интеграция с ИТ).

Вариант 1, 2.
Один или группа специалистов по ИБ внутри ИТ- департамента

Недостатки:

Консультационный режим работы.

Подчиненное положение по отношению к ИТ. ИБ рассматривается как часть ИТ, что не обеспечивает комплексности защиты (*вопросы работы с пользователями, безопасности информационных потоков, безопасности бизнес-процессов и другие организационные и юридические моменты остаются неучтенными, что снижает эффективность защиты*).

Остаточное финансирование.

Вариант 3, 4.
Один или группа специалистов по ИБ внутри службы безопасности

Преимущества:

Сравнительная простота реализации;
Более эффективное управление подразделением.
Возможность комплексного решения проблем ОИБ.

Вариант 3, 4.
Один или группа специалистов по ИБ внутри службы безопасности

Недостатки:

Консультационный режим работы.
Недооценка важности проблем ИБ непосредственным руководством.
Усложнение взаимодействия с ИТ-службой.
Остаточное финансирование.

Вариант 5
Один или несколько обособленных специалистов, подчиняющихся руководству предприятия

Преимущества:

Непосредственный контакт с топ-менеджментом.
Равноправное положение с другими подразделениями.

Вариант 5
Один или несколько обособленных специалистов, подчиняющихся руководству предприятия

Недостатки:

Отсутствие структуры, зависимость от чужих организационных ресурсов *(«подвешенное состояние»).*
Отсутствие собственной бюджетной статьи.
Сложность взаимодействия с другими подразделениями предприятия;

(Данный вариант не подходит для крупных организаций)

Вариант 6
Служба ИБ в виде независимой структуры, подчиняющейся руководству предприятия

Преимущества:

Непосредственный контакт с топ-менеджментом.
Наличие собственной структуры и организационных ресурсов.
Наличие собственной бюджетной статьи.
Равноправное положение с другими подразделениями.

Вариант 6
Служба ИБ в виде независимой структуры, подчиняющейся руководству предприятия

Недостатки:

Ресурсоемкость.
Сложность взаимодействия с ИТ-службой.

(Данный вариант не подходит для небольших организаций)

Основные источники возможных конфликтов

1. Противоречие функций службы ИБ и других подразделений;
2. Битвы за бюджет;
3. Внедрение требований ИБ;
4. Контроль требований ИБ;
5. Борьба за статус и последнее слово.

Вариант структуры Службы безопасности организации

Учёт персонала и информации
Разработка и организация пропускного режима

Охрана помещений
Охрана объектов
Личная охрана руководства
Личная охрана ведущих специалистов
Наблюдение за обстановкой вокруг и внутри объекта

Вариант структуры отдела ЗИ

Подразделение конфиденциального делопроизводства

- Обработка (получение, классификация, учет) и хранение конфиденциальных документов.
- Контроль системы конфиденциального документооборота.

Подразделение инженерно-технической защиты информации

Инженерно-техническая защита информации предназначена:

для активно-пассивного противодействия средствам технической разведки и формирования контуров охраны территории, помещений, оборудования с помощью технических средств и включает в себя:

- Средства физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здания и помещения.
- Средства нейтрализации технических каналов утечки информации при работе ЭВМ, средств связи, других ТС, при проведении совещаний и переговоров с посетителями и сотрудниками.
- Средства защиты помещений от визуальных способов технической разведки.
- Технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, технических средств и носителей информации.

Подразделение программно-аппаратной защиты информации

Задачи подразделения:

- Предотвращение несанкционированного доступа (НСД) к информации.
- Защита информации от вредоносных программ.
- Защита информации от сбоев в системе питания.
- Программно-аппаратная защита каналов передачи данных и взаимодействия с ССОП.

Информационно-аналитическое подразделение

Основными задачами подразделения являются:

- Сбор и оперативное использование информации в области гражданского, уголовного и хозяйственного законодательства (прежде всего в области ЗИ);
- Разработка и уточнение концепции информационной безопасности организации;
- Анализ внешних и внутренних угроз ИБ, поиск направлений их нейтрализации;
- Расследование инцидентов ИБ;
- Исследование (сравнительный анализ) существующих и перспективных средств защиты информации;
- Разработка проектов ОРД в области защиты информации и поддержание действующих документов в актуальном состоянии;
- Информирование сотрудников организации об изменении обязательных (государственных) требований по ОИБ (+ «просветительская работа»).

(Выявление угроз включает в себя не только сбор и добывание информации, ее обработку и анализ, но и подготовку конкретных предложений по их нейтрализации)

Периодичность организационно-технических мероприятий по ЗИ

Разовые (однократно проводимые и повторяемые только при пересмотре принятых решений);

Периодические (проводимые через определенное время);

Мероприятия, **проводимые по необходимости** (при возникновении изменений в защищаемой ИС или внешней среде);

Постоянно проводимые.

Основные мероприятия по ЗИ (ОИБ)

- подбор и подготовка должностных лиц (сотрудников), ответственных за организацию практических мероприятий по ИБ;

- учет подлежащих защите инф. ресурсов системы (информации, ее носителей, процессов обработки);

- разработка реально выполнимых и непротиворечивых ОРД по вопросам обеспечения безопасности информации;

- реализация (реорганизация) технологических процессов обработки информации (информационных потоков) с учетом требований по ИБ;

- принятие мер сохранности и физической целостности технических средств и носителей информации;

Основные мероприятия по ЗИ (ОИБ)

- регламентация доступа персонала к защищаемой информации;

- установление персональной ответственности каждого сотрудника, участвующего в рамках своих обязанностей в процессах обработки информации и имеющего доступ к инф. ресурсам;

- контроль за соблюдением пользователями и сотрудниками подразделения ИТ требований по обеспечению инф. безопасности;

- анализ эффективности принятых мер и применяемых СЗИ, разработка и реализация предложений по совершенствованию системы защиты информации.

Подразделение по защите информации на предприятии (в учреждении, организации)

- Подразделение по ЗИ является **самостоятельным структурным** подразделением. Штатная численность подразделения и его структура определяется руководителем организации.

- Непосредственное руководство работой подразделения по ЗИ осуществляет **заместитель руководителя**, ответственный за ЗИ.

- Подразделение по ЗИ может входить в состав одного из технических, научно-технических подразделений или в состав службы безопасности организации.

Подразделение по защите информации на предприятии (в учреждении, организации)

- Назначение и освобождение от должности руководителя подразделения по ЗИ производится руководителем организации **по согласованию с вышестоящей организацией, курирующей вопросы защиты информации**.

- На подразделение по ЗИ **запрещается** возлагать задачи, не связанные с его деятельностью.

Основные функции подразделения по защите информации:

1. Планирование работ по ЗИ;

2. Участие в подготовке предприятия к аттестованию на право проведения работ с использованием сведений, отнесенных к государственной тайне;

3. Организация разработки нормативно-методических документов по ЗИ;

4. Определение демаскирующих признаков предприятия, видов и средств иностранной технической разведки, технических каналов утечки информации, возможности несанкционированного доступа к информации и разработка соответствующих мер по ЗИ;

Основные функции подразделения по защите информации:

5. Разработка проектов распорядительных документов по вопросам организации ЗИ.

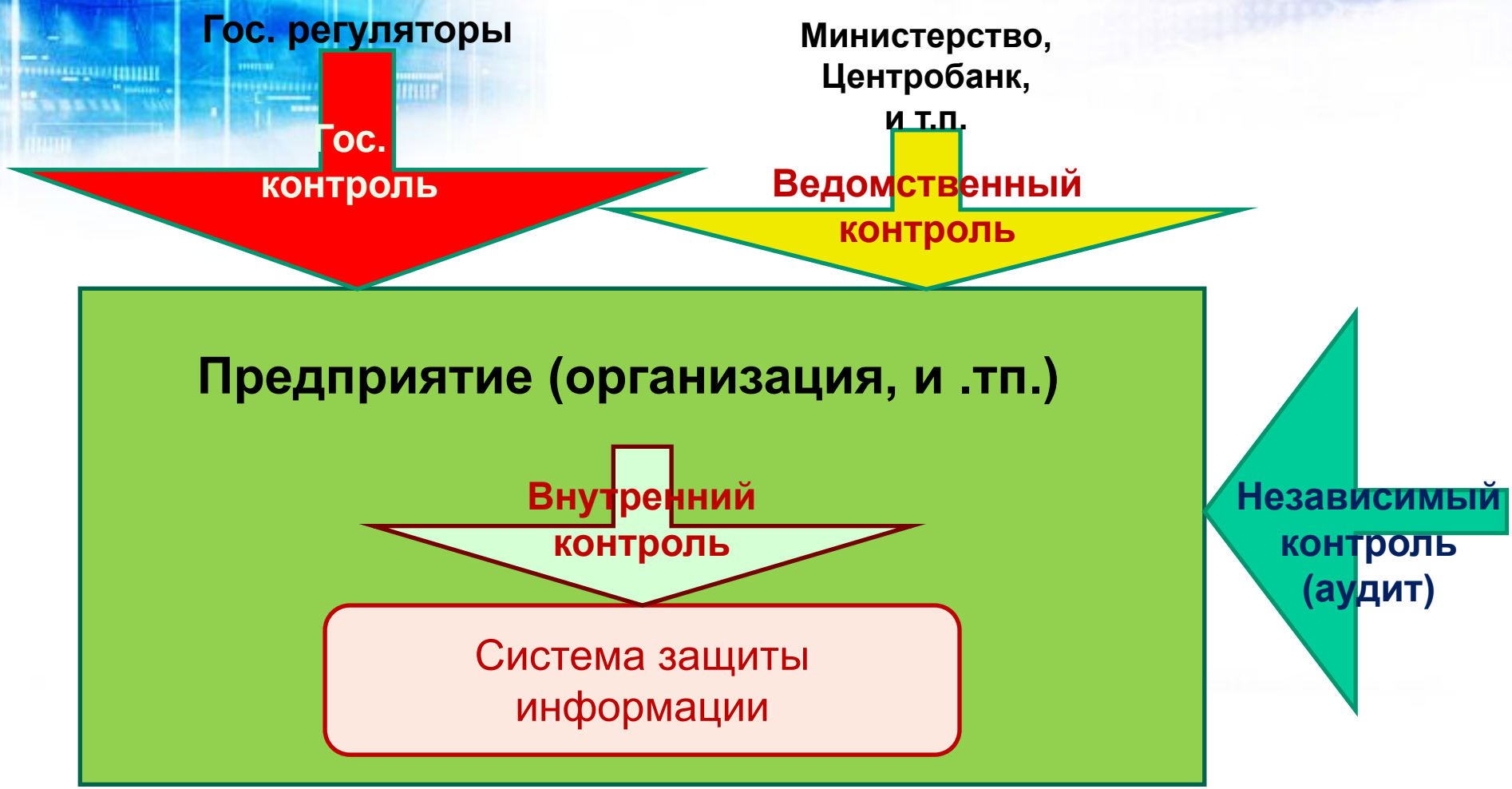
6. Организация специальных проверок и проведение аттестования рабочих мест, стендов, вычислительных комплексов (средств) и т.д. и выдача предписания на право проведения на них работ с секретной информацией (при наличии лицензии);

7. Разработка Руководства по ЗИ;

8. Подготовка отчетов о состоянии работ по ЗИ;

9. Организация проведения занятий с руководящим составом и специалистами предприятия по вопросам ЗИ.

Уровни контроля эффективности ЗИ



Государственный контроль (надзор)

Лицензионный контроль проводится лицензирующим органом.

Цели:

- проверка полноты и достоверности сведений о соискателе лицензии, содержащихся в представленных соискателем лицензии заявлении и документах;
- проверка возможности выполнения лицензиатом требований и условий при осуществлении лицензируемого вида деятельности;
- проверка сведений о лицензиате и соблюдения им лицензионных требований и условий при осуществлении лицензируемого вида деятельности.

*Проверка проводится лицензирующим органом в соответствии с требованиями Федерального закона **№294-ФЗ.** В отношении лицензиата и соискателя лицензии могут проводиться плановые и внеплановые, документарные или выездные проверки.*

ФЗ «О лицензировании отдельных видов деятельности»
*от 4 мая 2011 г. **№ 99**-ФЗ*

Государственный контроль (надзор)

Контроль и надзор за полнотой и качеством проводимых лицензиатами работ в области защиты информации осуществляет:

- ФСТЭК России;
- ФСБ России;
- отраслевые органы контроля в пределах их компетенции.

КОГДА?

- В ходе плановых проверок состояния защиты информации на предприятиях-потребителях, воспользовавшихся услугами лицензиатов.

- При контроле государственными органами по лицензированию качества выполненных лицензиатами работ по рекламациям предприятий-потребителей.

Государственный контроль (надзор)

Инспекционный контроль за сертифицированными средствами защиты информации осуществляют органы, проводившие сертификацию этих средств ЗИ.

При возникновении спорных вопросов в деятельности участников сертификации заинтересованная сторона может подать апелляцию:
- в орган по сертификации средств защиты информации,
- в федеральный орган по сертификации,
- в Межведомственную комиссию.

Указанные организации в месячный срок рассматривают апелляцию с привлечением заинтересованных сторон и извещают подателя апелляции о принятом решении.

Положение о сертификации средств защиты информации
Утверждено постановлением Правительства РФ от 26 июня 1995 г. № 608

Государственный контроль (надзор)

Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится ФСТЭК как в процессе, так и по завершении аттестации, **а за эксплуатацией аттестованных объектов информатизации** - периодически в соответствии с планом работы по контролю и надзору.

- ФСТЭК может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.
- Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

Положение по аттестации объектов информатизации по требованиям безопасности информации

Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

Государственный контроль (надзор)

Государственный контроль и надзор за соблюдением правил аттестации включает

- проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации,
- проверку правильности оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний,
- своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

Положение по аттестации объектов информатизации по требованиям безопасности информации
Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

Типовые нарушения по организации защиты информации

- Отсутствие штатных подразделений (специалистов) по защите информации;
- Отсутствие или некачественная разработка Руководства и Положения о порядке организации и проведения работ по защите конфиденциальной информации;
- Неправильное категорирование ОВТ;
- Неправильная классификация АС;
- Обработка секретной информации на несертифицированных средствах вычислительной техники и неаттестованных по требованиям безопасности информации объектах информатизации;

Типовые нарушения по организации защиты информации

- В выделенных (защищаемых) помещениях установлены ВТСС зарубежного производства, не прошедшие специальной проверки;
- Выделенные (защищаемые) помещения не аттестованы по требованиям безопасности информации;
- Невыполнение требований по защите конфиденциальной информации, циркулирующей в автоматизированных системах (автономных ПЭВМ и ЛВС).