МЕРОПРИЯТИЯ ПО ВВОДУ В ДЕЙСТВИЕ ТРЕБОВАНИЙ ГОСТ Р ИСО/МЭК 27001-2006

Гордеев Сергей

специалист по защите информации

ОАО ПКО «Теплообменник»

УДОБНО!

- Телекоммуникационные устройства;
- Облачные сервисы;
- Переносные устройства (внешние диски, флешки, карты MicroSD, SD и т.п.);
- Социальные сети и различные агенты общения.

- **ПРАВДА УДОБНО?!**

УДОБНО, НО ДЛЯ КОГО?!

- Практически все устройства имеют не декларированные возможности (прослушивание, слежение, скрытая передача информации);
- Облака бесплатные, но бесплатный сыр только в мышеловке! Сервера практически все находятся за пределами России;
- Использование домашней техники для работы с рабочей информацией. НЕТ ГАРАНТИИ «ЧИСТОТЫ» ВАШЕЙ ДОМАШНЕЙ ТЕХНИКИ;
- Что, после работы, пишут ваши сотрудники в социальных сетях и агентах?

Угрозы «Человеческого фактора»

- Порча репутации организации;
- Подмена информации;
- Уничтожение информации;
- Потеря информации (физическая);
- **Потеря конкурентоспособности на рынке = СМЕРТЬ ОРГАНИЗАЦИИ**

Внешние угрозы

- Деятельность иностранных, политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- Стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению её с внешнего и внутреннего информационных рынков;

Внешние угрозы

- Разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Внутренние угрозы

- Уничтожение, повреждение, разрушение или хищение цифровых и других носителей информации;
- Перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- Использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

Внутренние угрозы

- Несанкционированный доступ к информации, находящейся в хранилищах информации;
- Нарушение законных ограничений на распространение информации.

Сказка о флешке

- В городе Н. регуляторы решили проверить безопасность одной организации, а дело было к обеду …

1 января 2013 года наступило время «Ч»

Вступил в силу Государственный военный стандарт

ГОСТ РВ 0015-002-2012 (ДСП)

Система разработки и постановки на производство военной техники

СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

Общие требования

4.3 «Обеспечение информационной безопасности»

- **4.3.1** ***В организации должен быть определён и документально оформлен порядок организации и выполнения работ по защите информации об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа…***

4.3 «Обеспечение информационной безопасности»

- 4.3.2 *В организации должно быть **определено подразделение (ответственный), осуществляющее менеджмент информационной безопасности** на всех этапах жизненного цикла военной продукции.*

4.3 «Обеспечение информационной безопасности»

☹ **4.3.3** ***При наличии соответствующих требований в контрактах (договорах) в организации должен быть определён и документально оформлен порядок выполнения работ по обеспечению информационной безопасности в соответствии с требованиями стандарта ГОСТ Р ИСО/МЭК 27001.***

А оно нам надо?

- 4.3.3 *При наличии соответствующих требований в контрактах (договорах) в организации…*

- Пока этого требования в контрактах нет, **но только пока…**

А завтра ...?

Не брать заказ?!

Уже сегодня… из системы «Консультант Плюс»

- **Типовой договор на выполнение работ по монтажу и наладке компьютерных сетей**
- … <1> Основные требования к Сети и документации содержат: ст. 9 ГОСТ Р 53246-2008. Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования (утв. Приказом Ростехрегулирования от 25.12.2008 N 786-ст), ***ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности…***

Вывод:

следует уже сегодня начать внедрение ИСО 27001.

Что такое информационная безопасность?

- Пункт 3.4 Информационная безопасность – это свойство информации сохранять конфиденциальность, целостность и доступность.

Что такое система менеджмента информационной безопасности?

- Пункт 3.7 СМИБ. Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

1.2 Примечание

- Требования, устанавливаемые настоящим стандартом, предназначены для применения во всех организациях независимо от типа, масштабов и сферы деятельности. **Исключение любого из требований, указанных в разделах 4, 5, 6, 7, 8 – не допускается, если организация заявляет о соответствии её СМИБ настоящему стандарту.**

1.2 Примечание

- Любой отказ от применения той или иной меры управления, обусловленный необходимостью удовлетворения критериев принятия рисков, **должен быть обоснован**. Необходимо также наличие адекватных доказательств того, что подобные риски были уже **приняты ответственными лицами и официально утверждены высшим руководством**.

Объекты СМИБ

- Являются все информационные активы организации:
- Бумажные и электронные документы;
- Вычислительная техника;
- Информационные системы;

- Технологические каналы информации (сети, связь, доставка курьером, охраняемый периметр и т.п.);
- Персонал, хранящий и обрабатывающий информацию в своих головах и рабочих местах.

Что получим в итоге от СМИБ?

- Выявление наиболее опасных угроз и экономия средств на создание эффективной системы обеспечения информационной безопасности.
- Расследование инцидентов.
- Порядок и контроль над информационными потоками организации.

Информационная безопасность – это компромисс между защитой и финансовой выгодой.

Единственная цель организации – получение финансовой выгоды!

Внедрение СМИБ

- 1 ступень - Управленческая
- 2 ступень – Определение направления защиты
- 3 ступень – Реализация мер защиты

1-ая ступень - Управленческая

- 1.1 Организационная структура и ответственность за ИБ;
- 1.2 Управление ресурсами;
- **1.3 Управление рисками;**
- 1.4 Управление документацией;
- 1.5 Внутренние аудиты;
- 1.6 Анализ системы высшим руководством;
- 1.7 Улучшение системы.

2-ая ступень. Определение направления защиты

- Определение чётких направлений информационной безопасности.
- Приложение А.
- Направлений 131.
- Сгруппированы в 11 этапов.

Этап 1.

Политика информационной безопасности

2-ая ступень. Определение направления защиты

- *ЭТАП 1. Политика информационной безопасности*
- ***Документирование политики ИБ***

- **Политика ИБ должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций.**

2-ая ступень. Определение направления защиты

- *ЭТАП 1. Политика информационной безопасности*
- ***Анализ политики ИБ***
- Политика ИБ должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности.

Этап 2.

Организация информационной безопасности

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***
- ***Внешняя организация***

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Обязанности руководства по обеспечению ИБ - Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путём внедрения СМИБ, распределения обязанностей и ответственности персонала за её обеспечение;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Координация вопросов обеспечения ИБ - Действия по обеспечению ИБ должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Распределение обязанностей по обеспечению ИБ - Обязанности персонала по обеспечению ИБ должны быть чётко определены;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Процедура получения разрешения на использование средств обработки информации - Руководство должно определить и внедрить процедуры получения разрешения на использование новых средств обработки информации;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Соглашения о соблюдении конфиденциальности - Руководство организации должно определять условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Взаимодействие с компетентными органами - Руководство организации должно поддерживать взаимодействие с соответствующими компетентными органами;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внутренняя организация***

Независимая проверка (аудит) информационной безопасности - Порядок организации и управления информационной безопасностью и её реализация (например, изменение целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определённые промежутки времени или при появлении существенных изменений в способах реализации мер безопасности;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внешняя организация***

Определение рисков, связанных со сторонними организациями - Перед предоставлением доступа сторонним организациям к информации и средствам её обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности;

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внешняя организация***

Рассмотрение вопросов безопасности при работе с клиентами - Перед предоставлением клиентам права доступа к информации или активам организации необходимо определить и внедрить меры безопасности.

2-ая ступень. Определение направления защиты

- *ЭТАП 2. Организация информационной безопасности*
- ***Внешняя организация***

Рассмотрение требований безопасности в соглашениях со сторонними организациями - Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации.

Этап 3.

Управление активами

2-ая ступень. Определение направления защиты

- *ЭТАП 3. Управление активами*
- ***Ответственность за защиту активов организации***

Инвентаризация активов - Опись всех важных активов организации должна быть составлена и актуализирована;

2-ая ступень. Определение направления защиты

- *ЭТАП 3. Управление активами*
- ***Ответственность за защиту активов организации***

Владение активами - Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение представителя организации;

2-ая ступень. Определение направления защиты

- *ЭТАП 3. Управление активами*
- ***Ответственность за защиту активов организации***

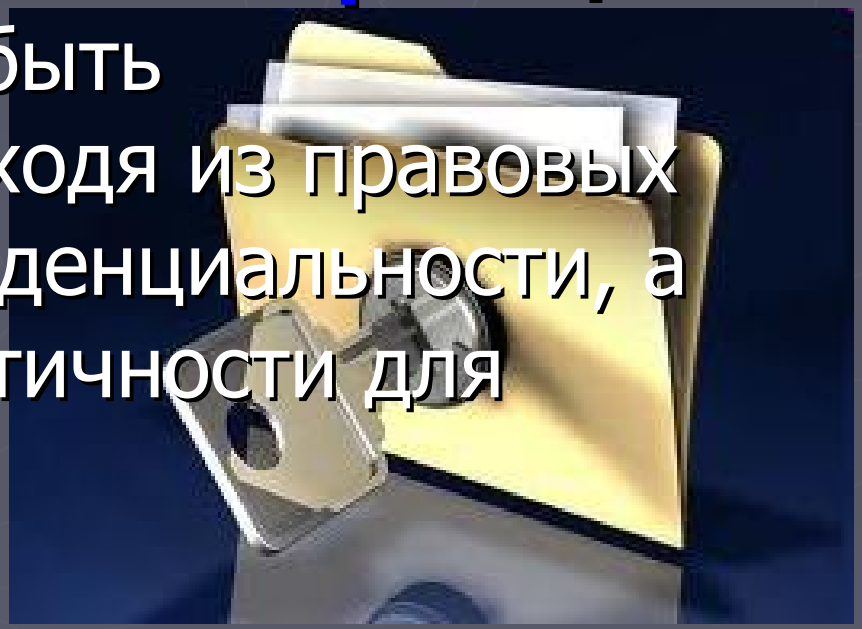
Приемлемое использование активов - Правила безопасного использования информации и активов, связанных со средствами обработки информации, должны быть определены, документированы и реализованы;

2-ая ступень. Определение направления защиты

- *ЭТАП 3. Управление активами*

- ***Классификация информации***

Основные принципы классификации - Информация должна быть классифицирована исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации;



2-ая ступень. Определение направления защиты

- *ЭТАП 3. Управление активами*

- ***Классификация информации***

Маркировка и обработка информации - В соответствии с принятой в организации системой классификации должна быть разработана и реализована совокупность процедур маркировки и обработки информации.

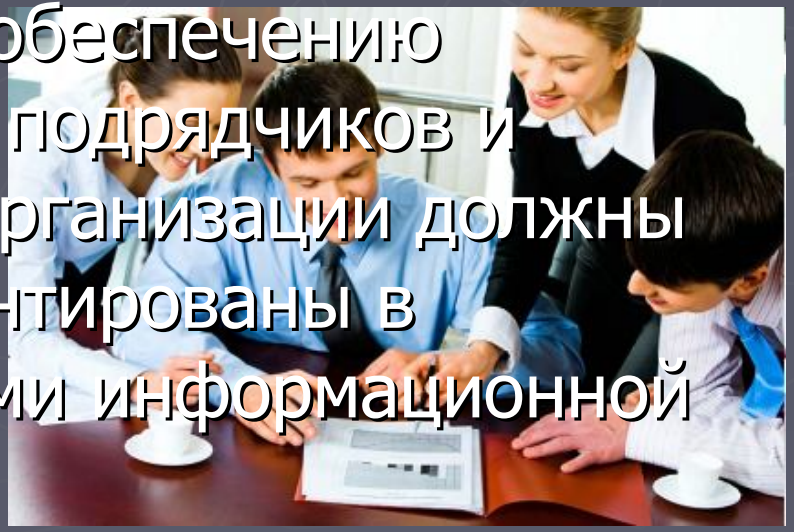
Этап 4.

Правила безопасности связанные с персоналом

2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Перед трудоустройством***

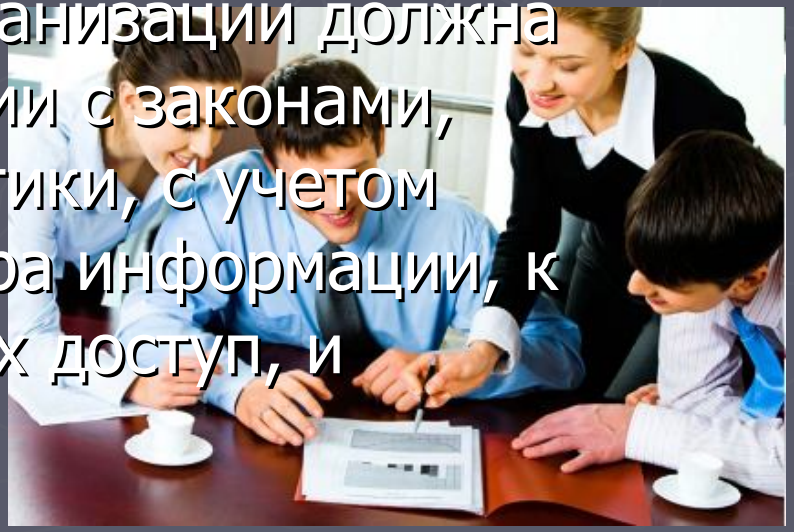
Функции и обязанности персонала по обеспечению безопасности - Функции и обязанности персонала по обеспечению безопасности сотрудников, подрядчиков и пользователей сторонней организации должны быть определены и документированы в соответствии с требованиями информационной безопасности;



2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Перед трудоустройством***

Проверка при приёме на работу - Проверка всех кандидатов на постоянную работу, подрядчиков и пользователей сторонней организации должна быть проведена в соответствии с законами, инструкциями и правилами этики, с учетом требований бизнеса, характера информации, к которой будет осуществлен их доступ, и предполагаемых рисков;



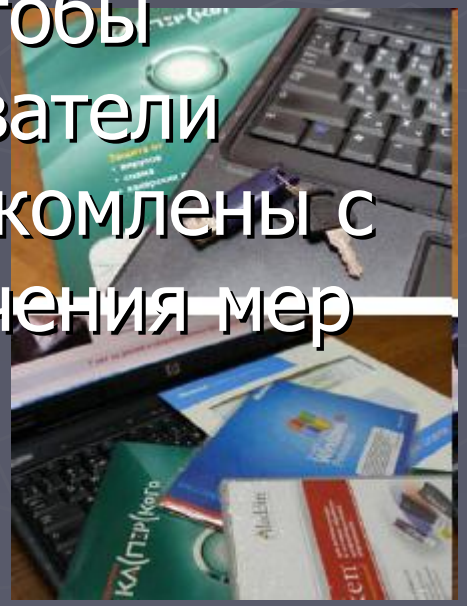
2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Перед трудоустройством***

Условия трудового договора - Сотрудники, подрядчики и пользователи сторонней организации должны согласовать и подписать условия своего трудового договора, в котором установлены их ответственность и ответственность организации относительно информационной безопасности.

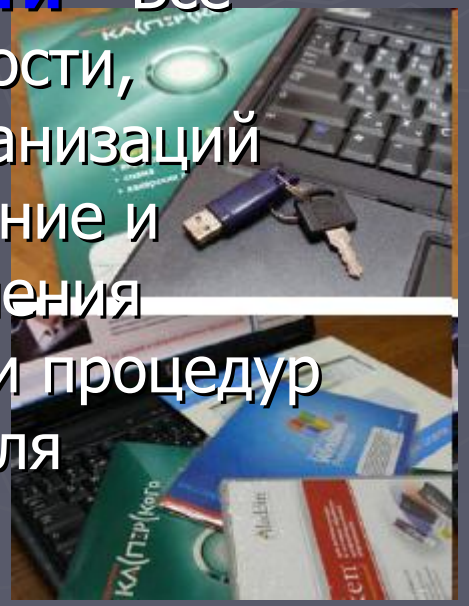
2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Работа по трудовому договору***
- **Обязанности руководства -** Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями;



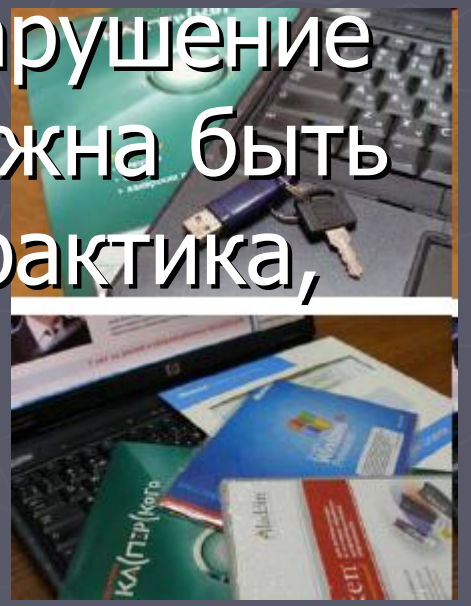
2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Работа по трудовому договору***
- **Осведомленность, обучение и переподготовка в области информационной безопасности -** Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций;



2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*
- ***Работа по трудовому договору***
- **Дисциплинарная практика -** К сотрудникам, совершившим нарушение требований безопасности, должна быть применена дисциплинарная практика, установленная в организации.

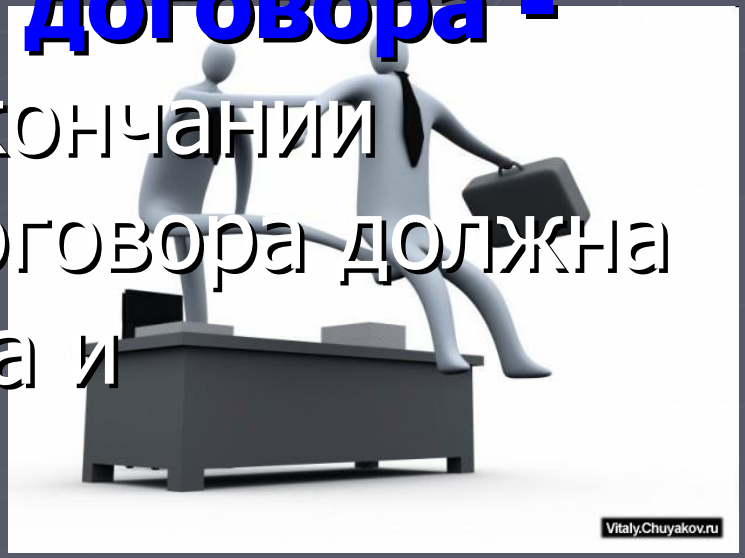


2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*

Увольнение или изменение трудового договора

- **Ответственность по окончании действия трудового договора -** Ответственность по окончании действия трудового договора должна быть четко определена и установлена;

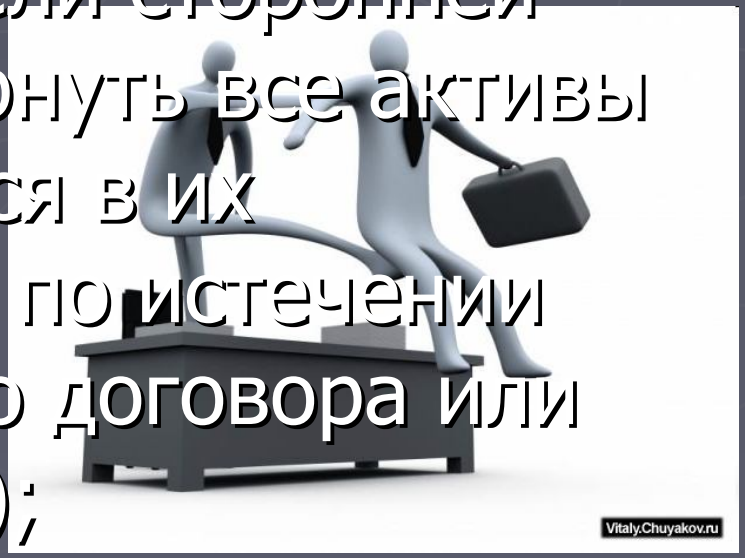


2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*

Увольнение или изменение трудового договора

- **Возврат активов -** Сотрудники, подрядчики и пользователи сторонней организации обязаны вернуть все активы организации, находящиеся в их пользовании (владении), по истечении срока действия трудового договора или соглашения (увольнение);

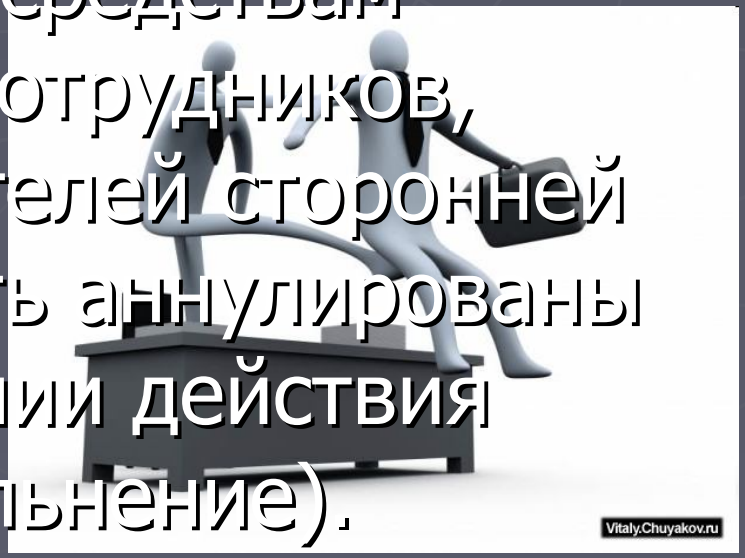


2-ая ступень. Определение направления защиты

- *ЭТАП 4. Правила безопасности связанные с персоналом*

Увольнение или изменение трудового договора

- **Аннулирование прав доступа -** Права доступа к информации и средствам обработки информации сотрудников, подрядчиков и пользователей сторонней организации должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение).



Этап 5.

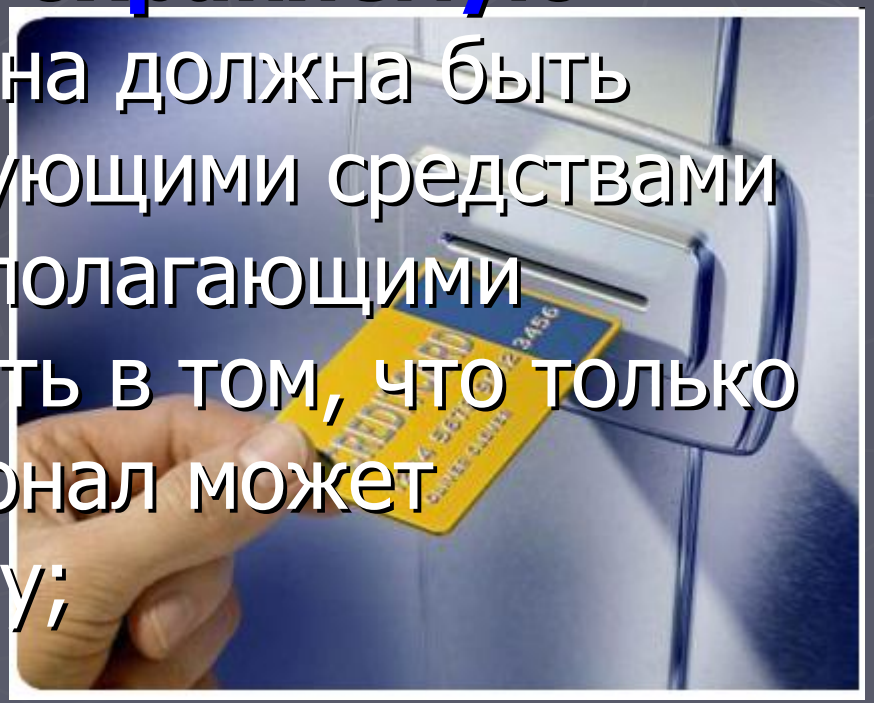
Физическая защита и защита от воздействия окружающей среды

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Периметр охраняемой зоны -** Для защиты зон, где имеются информация и средства обработки информации, должны быть использованы периметры охраняемых зон (барьеры, такие как стены, проходные, оборудованные средствами контроля входа по идентификационным карточкам, или, где предусмотрен, контроль сотрудника регистрационной стойки).

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Контроль доступа в охраняемую зону -** Охраняемая зона должна быть защищена соответствующими средствами контроля входа, предполагающими обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону;

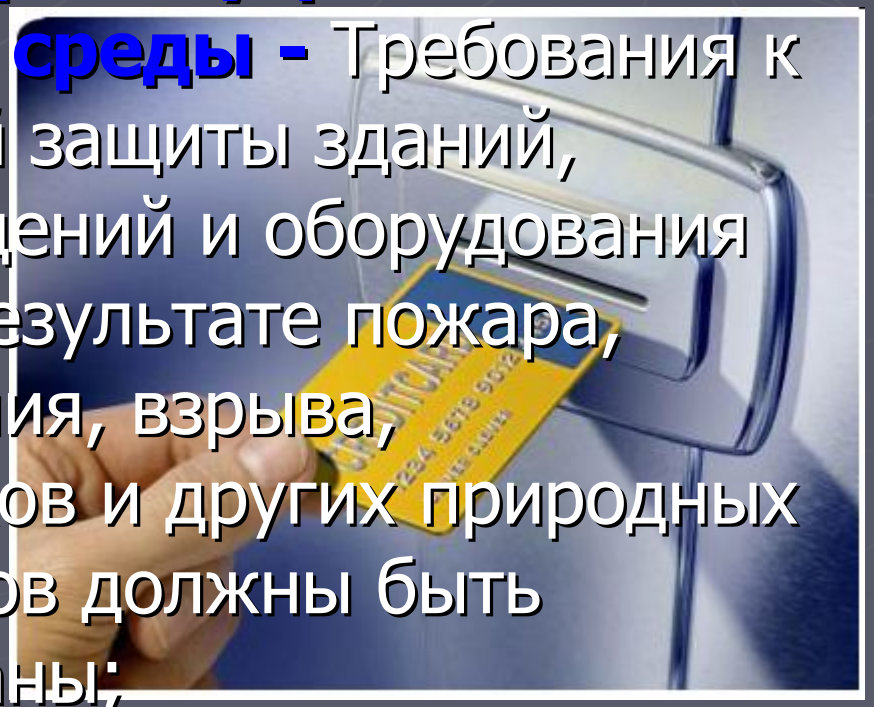


2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Обеспечение безопасности зданий, производственных помещений и оборудования -** Требования к обеспечению физической безопасности зданий, производственных помещений и оборудования должны быть разработаны и реализованы;

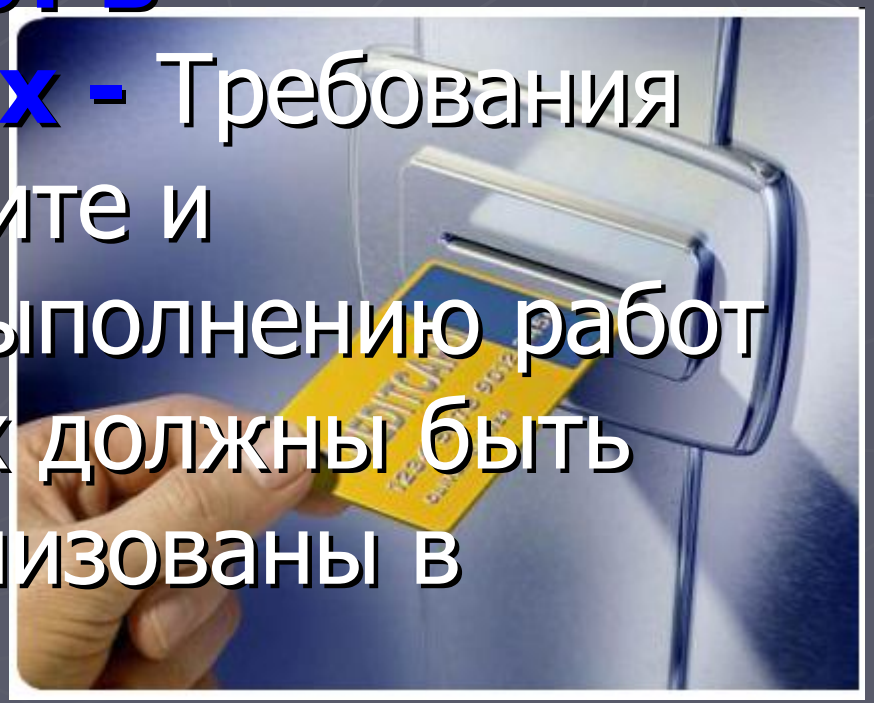
2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Защита от внешних угроз и угроз со стороны окружающей среды -** Требования к обеспечению физической защиты зданий, производственных помещений и оборудования от нанесения ущерба в результате пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других природных и антропогенных факторов должны быть разработаны и реализованы;



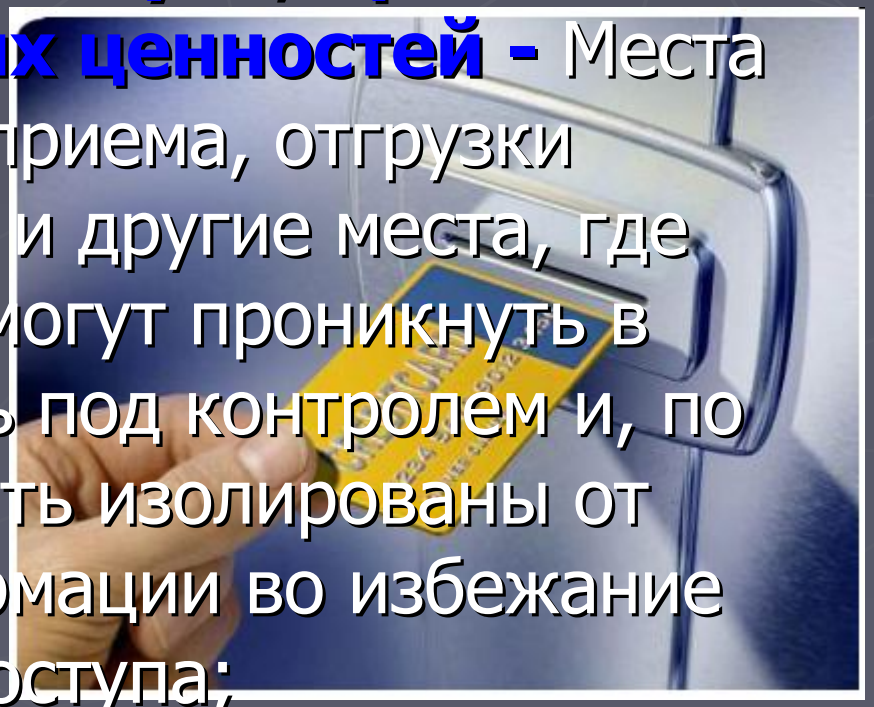
2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Выполнение работ в охраняемых зонах -** Требования по физической защите и рекомендации по выполнению работ в охраняемых зонах должны быть разработаны и реализованы в инструкциях;



2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Охраняемые зоны***
- **Зоны общественного доступа, приёма и отгрузки материальных ценностей -** Места доступа, такие как зоны приема, отгрузки материальных ценностей и другие места, где неавторизованные лица могут проникнуть в помещения, должны быть под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа;



2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Размещение и защита оборудования** - Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа;

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Размещение и защита оборудования** - Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа;

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Вспомогательные услуги -** Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами в обеспечении вспомогательных услуг;

2-ая ступень. Определение направления защиты

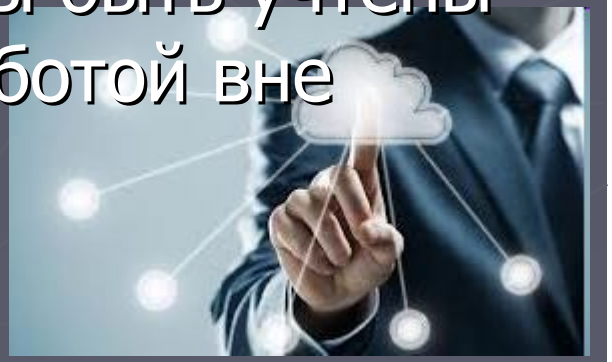
- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Безопасность кабельной сети -** Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, необходимо защищать от перехвата информации или повреждения;

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Техническое обслуживание оборудования -** Должно проводиться надлежащее регулярное техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и сохранности;

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Обеспечение безопасности оборудования, используемого вне помещений организации -** При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны быть учтены различные риски, связанные с работой вне помещений организации;



2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Безопасная утилизация или повторное использование оборудования -** Все компоненты оборудования, содержащие носители данных, должны быть проверены с целью удостовериться в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или скопированы безопасным образом до их утилизации (списания);

2-ая ступень. Определение направления защиты

- *ЭТАП 5. Физическая защита и защита от воздействия окружающей среды*
- ***Безопасность оборудования***
- **Вынос имущества с территории организации -** Оборудование, информацию или программное обеспечение допускается выносить из помещения организации только на основании соответствующего разрешения.

Этап 6.

Управление средствами коммуникаций и их функционированием

2-ая ступень. Определение направления защиты

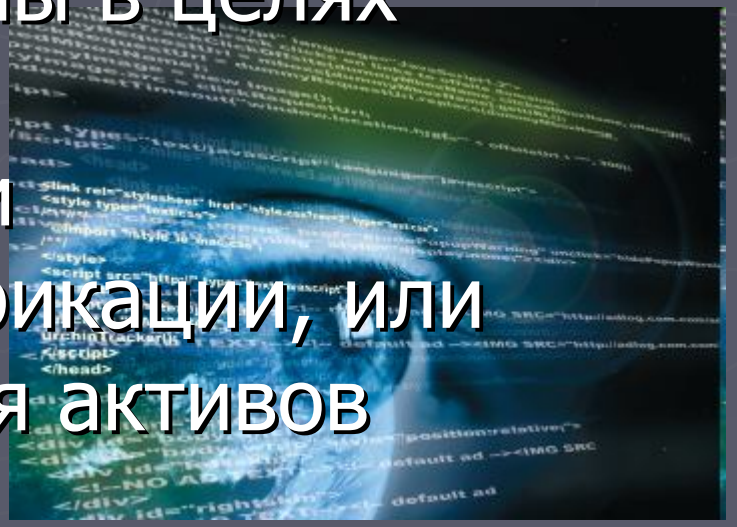
- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Эксплуатация средств и ответственность***
- **Документирование операционных процедур эксплуатации -** Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Эксплуатация средств и ответственность***
- **Управление изменениями -** Изменения в конфигурациях средств обработки информации и системах должны быть контролируемыми;

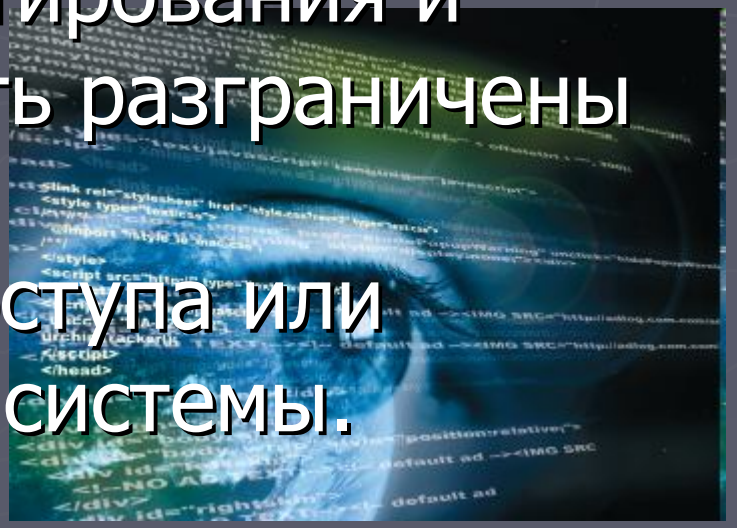
2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Эксплуатация средств и ответственность***
- **Разграничение обязанностей -** Обязанности и области ответственности должны быть разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации, или нецелевого использования активов организации;



2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Эксплуатация средств и ответственность***
- **Разграничение средств разработки, тестирования и эксплуатации -** Средства разработки, тестирования и эксплуатации должны быть разграничены в целях снижения риска несанкционированного доступа или изменения операционной системы.



2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Управление поставкой услуг лицами и/или сторонними организациями***
- **Оказание услуг** - Должна быть обеспечена уверенность в том, что меры управления информационной безопасностью, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Управление поставкой услуг лицами и/или сторонними организациями***
- **Изменения при оказании сторонними организациями услуг по обеспечению безопасности -** Изменения при оказании услуг по обеспечению безопасности, включая внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков.

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Планирование производительности и загрузки систем***
- **Управление производительностью –** Отчёты о работе систем, потреблении мощностей, прогнозы роста;
- **Приёмка систем –** требования к системам, их приём, пробная эксплуатация на «кроликах», тестовая эксплуатация, параллельное ведение системы (старая, новая), полный ввод в действие новой (изменённой).

2-ая ступень. Определение направления защиты

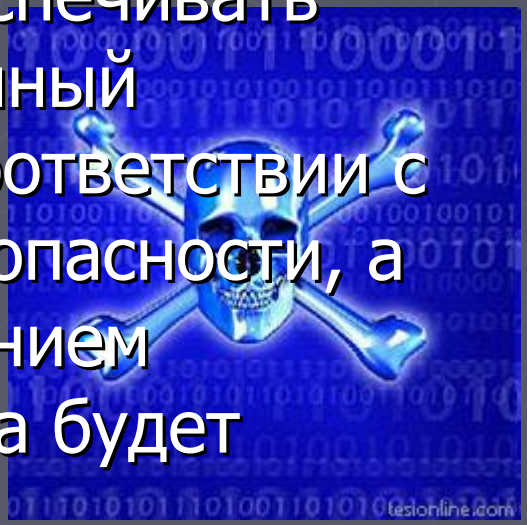
- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Защита от вредоносного кода и мобильного кода***

- **Меры защиты от вредоносного кода -** Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Защита от вредоносного кода и мобильного кода***

- **Меры защиты от мобильного кода -** Там, где разрешено использование мобильного кода, конфигурация системы должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операции с использованием неавторизованного мобильного кода будет предотвращено.



2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Резервирование***

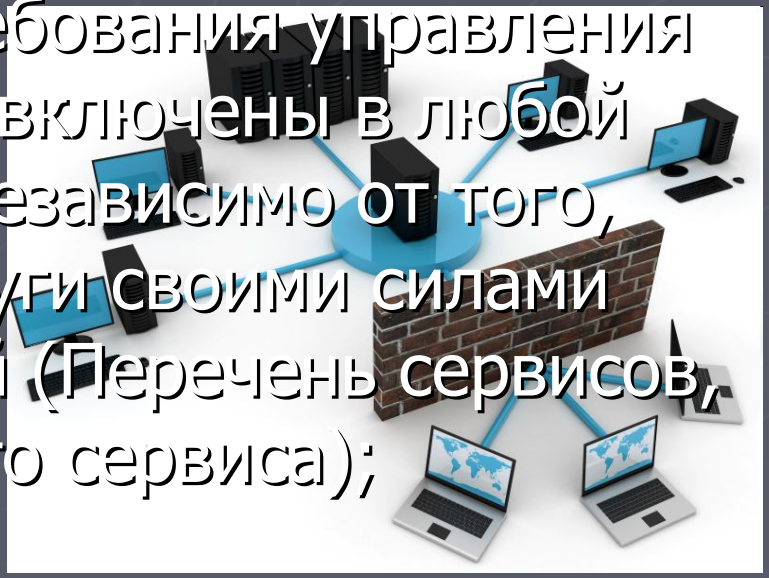
- **Резервирование информации -** Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования.

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Управление безопасностью сети***
- **Средства контроля сети –** сеть должна быть адекватно защищена (Требования к защите);

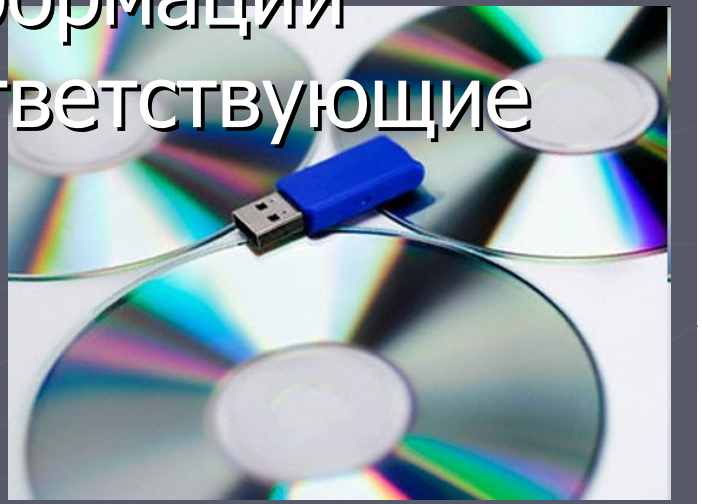
2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Управление безопасностью сети***
- **Безопасность сетевых сервисов -** Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией (Перечень сервисов, требования к защите каждого сервиса);



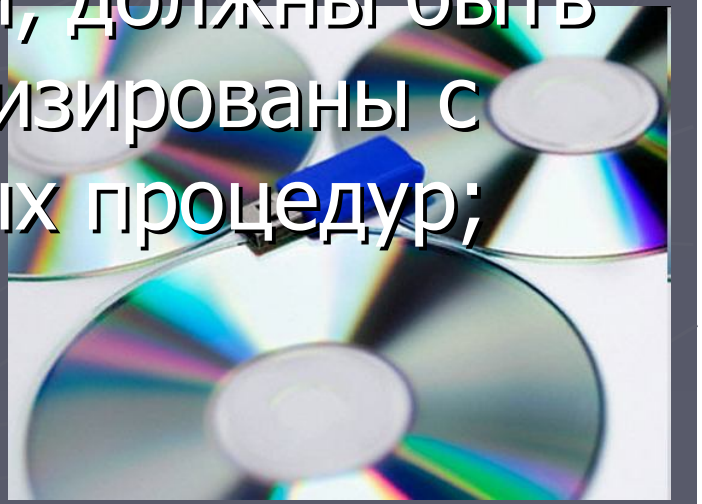
2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обращение с носителями информации***
- **Управление съёмными носителями информации** - Для управления съёмными носителями информации должны существовать соответствующие процедуры;



2-ая ступень. Определение направления защиты

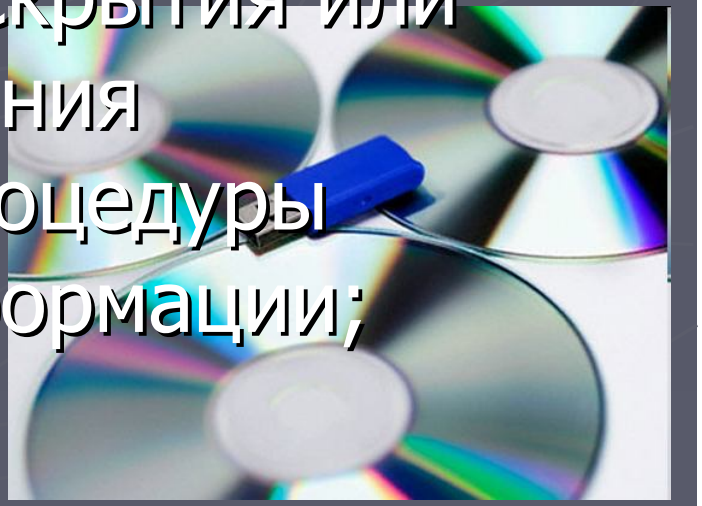
- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обращение с носителями информации***
- **Утилизация носителей информации -** Носители информации, когда в них больше нет необходимости, должны быть надежно и безопасно утилизированы с помощью формализованных процедур;



2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обращение с носителями информации***
- **Процедуры обработки информации**

-Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования необходимо установить процедуры обработки и хранения информации;



2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обращение с носителями информации***
- **Безопасность системной документации -** Системная документация должна быть защищена от несанкционированного доступа.

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обмен информацией***
- **Политики и процедуры обмена информацией -** Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обмен информацией***
- **Соглашения по обмену информацией -**Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обмен информацией***
- **Защита физических носителей информации при транспортировке**
  -Носители информации должны быть защищены от несанкционированного доступа, неправильного использования или повреждения во время их транспортировки за пределами территории организации;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обмен информацией***
- **Электронный обмен сообщениями -** Информация, используемая в электронном обмене сообщениями, должна быть защищена надлежащим образом;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Обмен информацией***
- **Системы бизнес-информации -** Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации.

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Услуги электронной торговли***
- **Электронная торговля -** Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации;

2-ая ступень. Определение направления защиты

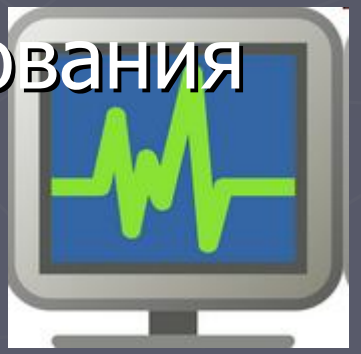
- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Услуги электронной торговли***
- **Трансакции в режиме реального времени -** Информация, используемая в трансакциях в режиме реального времени, должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного воспроизведения сообщений.

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Мониторинг***
- **Ведение журналов аудита -** Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа;

2-ая ступень. Определение направления защиты

- *ЭТАП 6. Управление средствами коммуникаций и их функционирование*
- ***Мониторинг***
- **Мониторинг использования средств обработки информации -** Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации.



Этап 7.

Контроль доступа

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Бизнес-требования к контролю доступа***
- **Политика контроля доступа -** Политика контроля доступа должна быть установлена и документирована с учётом потребностей бизнеса и безопасности информации.

2-ая ступень. Определение направления защиты

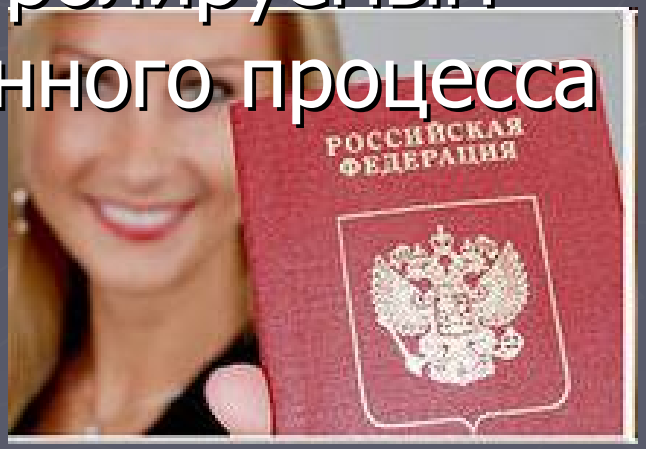
- *ЭТАП 7. Контроль доступа*
- ***Управление доступом пользователей***
- **Регистрация пользователей -** Должна быть установлена формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Управление доступом пользователей***
- **Управление привилегиями -** Предоставление и использование привилегий должно быть ограниченным и контролируемым;

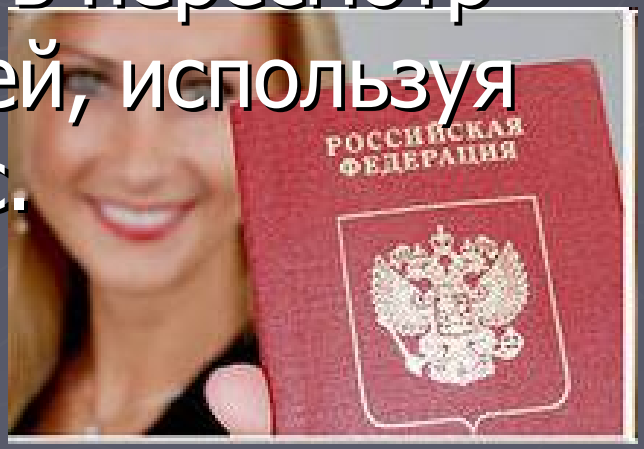
2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Управление доступом пользователей***
- **Управление паролями пользователей -** Предоставление паролей должно быть контролируемым посредством формализованного процесса управления;



2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Управление доступом пользователей***
- **Пересмотр прав доступа пользователей -** Руководство должно периодически осуществлять пересмотр прав доступа пользователей, используя формализованный процесс.



2-ая ступень. Определение направления защиты

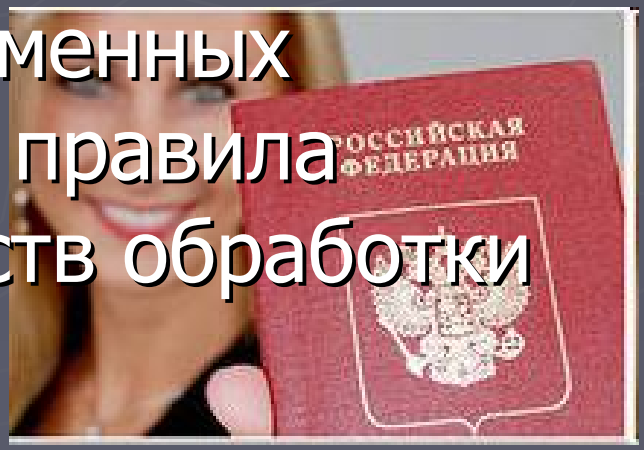
- *ЭТАП 7. Контроль доступа*
- ***Ответственность пользователей***
- **Использование паролей -** Пользователи должны соблюдать правила безопасности при выборе и использовании паролей;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Ответственность пользователей***
- **Оборудование, оставленное пользователем без присмотра -** Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Ответственность пользователей***
- **Правила «чистого стола» и «чистого экрана» -** Должны быть приняты правила «чистого стола» для документов на бумажных носителях и сменных носителей данных, а также правила «чистого экрана» для средств обработки информации.



2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Политика в отношении использования сетевых услуг - Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Аутентификация пользователей для внешних соединений - Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации;

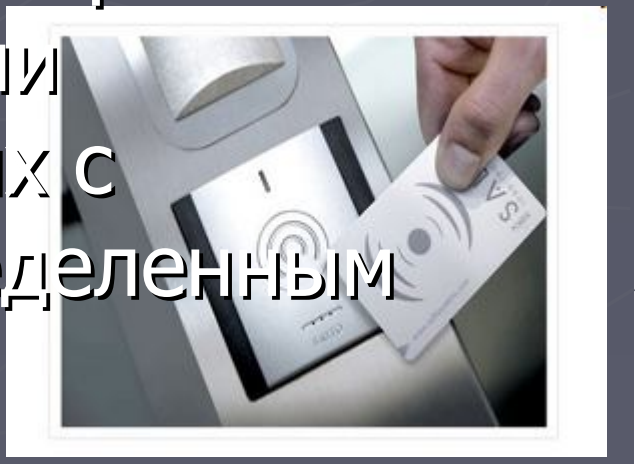
2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Идентификация оборудования в сетях

- Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием.



2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Защита диагностических и конфигурационных портов при удаленном доступе - Физический и логический доступ к портам конфигурации и диагностики должен быть контролируемым;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

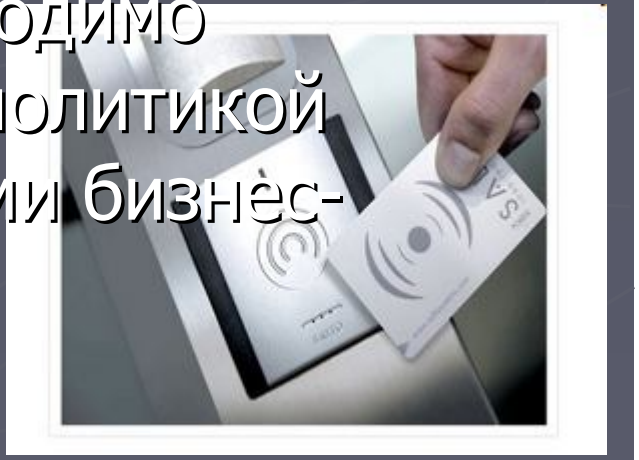
Принцип разделения в сетях - В сетях должны быть применены принципы разделения групп информационных услуг, пользователей и информационных систем;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Контроль сетевых соединений - Подключение пользователей к совместно используемым сетям, особенно к тем, которые выходят за территорию организации, необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений;

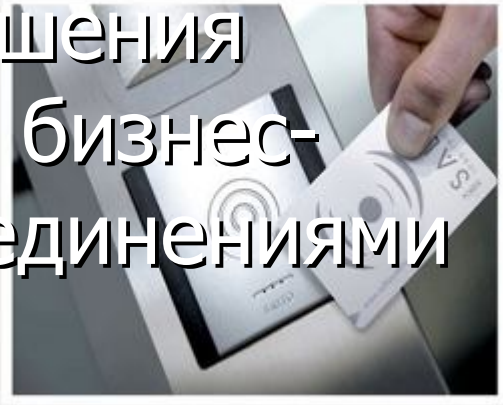


2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль сетевого доступа***

Контроль маршрутизации в сети - Должны быть внедрены средства управления и контроля маршрутизации в сети с целью исключить нарушения правил контроля доступа для бизнес-приложений, вызываемые соединениями и потоками информации.



2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*
- ***Контроль доступа к операционной системе***

Безопасные процедуры регистрации - Контроль доступа к операционным системам должен быть обеспечен безопасной процедурой регистрации;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к операционной системе***

Идентификация и аутентификация пользователя - Все пользователи должны иметь уникальные идентификаторы (ID) только для персонального использования, а для подтверждения заявленной личности пользователя должны быть выбраны подходящие методы аутентификации;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к операционной системе***

Система управления паролями -

Системы управления паролями должны быть интерактивными и обеспечивать высокое качество паролей;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к операционной системе***

Использование системных утилит - Использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений, необходимо ограничивать и строго контролировать;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к операционной системе***

Периоды бездействия в сеансах связи

- Необходимо обеспечить завершение сеансов связи после определенного периода бездействия;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к операционной системе***

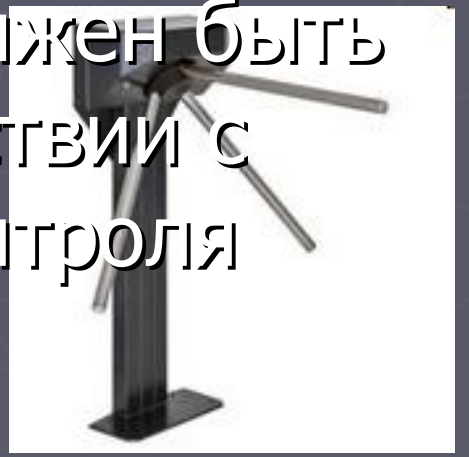
Ограничение времени соединения - Ограничение времени соединения должно быть использовано для обеспечения дополнительной безопасности.

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к прикладным системам и информации***

Ограничения доступа к информации - Доступ к информации и функциям прикладных систем пользователей и обслуживающего персонала должен быть предоставлен только в соответствии с определенными политиками контроля доступа;



2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Контроль доступа к прикладным системам и информации***

Изоляция систем, обрабатывающих важную информацию - Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду.

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Работа с переносными устройствами и работа в дистанционном режиме***

Работа с переносными устройствами - Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании переносных устройств;

2-ая ступень. Определение направления защиты

- *ЭТАП 7. Контроль доступа*

- ***Работа с переносными устройствами и работа в дистанционном режиме***

Работа в дистанционном режиме - Для работы в дистанционном режиме необходимо разработать и реализовать политику, оперативные планы и процедуры.

Этап 8.

Разработка, внедрение и обслуживание информационных систем

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Требования к безопасности информационных систем***

Анализ и детализация требований безопасности - В формулировках требований бизнеса для новых информационных систем или совершенствования существующих должны быть детализированы требования безопасности;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Правильная обработка данных в приложениях***

Проверка достоверности входных данных - Входные данные для приложений должны быть подвергнуты процедуре подтверждения с целью установления их достоверности;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Правильная обработка данных в приложениях***

Контроль обработки данных в приложениях - Для обнаружения искажений (ошибок или преднамеренных действий) при обработке информации в требования к функциям приложений должны быть включены требования по выполнению контрольных проверок;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Правильная обработка данных в приложениях***

Целостность сообщений - Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также реализованы соответствующие средства контроля.

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Правильная обработка данных в приложениях***

Подтверждение достоверности выходных данных - Данные, выводимые из приложения, необходимо подвергать проверке на корректность, чтобы обеспечить уверенность в том, что обработка информации выполнена правильно.

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Криптографические средства защиты***

Политика использования криптографических средств защиты - Должны быть разработаны и внедрены правила использования криптографических средств защиты информации;

Aladdin
SECURING THE GLOBAL VILLAGE

КРИПТО ПРО

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Криптографические средства защиты***

Управление ключами - Для реализации организацией криптографических методов защиты должна быть использована система управления ключами.

Aladdin®
SECURING THE GLOBAL VILLAGE

КРИПТО ПРО

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Безопасность системных файлов***

Контроль программного обеспечения, находящегося в промышленной эксплуатации - Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Безопасность системных файлов***

Защита данных тестирования системы

- Данные тестирования следует тщательно отбирать, защищать и контролировать;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Безопасность системных файлов***

Контроль доступа к исходным кодам - Доступ к исходным кодам должен быть ограничен;

2-ая ступень. Определение направления защиты

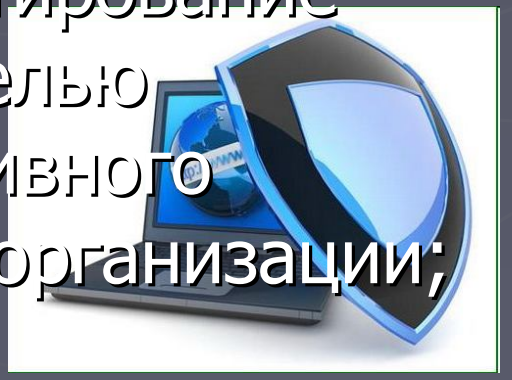
- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Безопасность в процессах разработки и поддержки***

Процедуры контроля изменений - Внесение изменений должно быть проверено с использованием соответствующих формализованных процедур контроля изменений;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Безопасность в процессах разработки и поддержки***

Технический анализ прикладных систем после внесения изменений в операционные системы - При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации;



2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Безопасность в процессах разработки и поддержки***

Ограничения на внесение изменений в пакеты программ - Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю;

2-ая ступень. Определение направления защиты

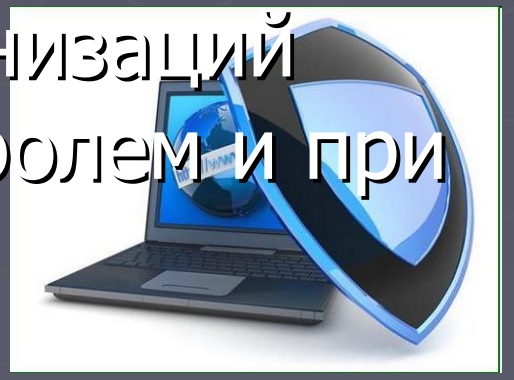
- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Безопасность в процессах разработки и поддержки***

Утечка информации - Возможности для утечки информации должны быть предотвращены;

2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*
- ***Безопасность в процессах разработки и поддержки***

Разработка программного обеспечения с привлечением сторонних организаций - Разработка программного обеспечения с привлечением сторонних организаций должна проводиться под контролем и при мониторинге организации.



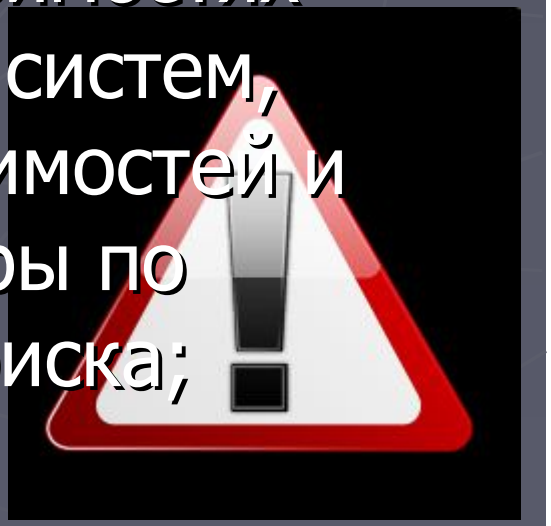
2-ая ступень. Определение направления защиты

- *ЭТАП 8. Разработка, внедрение и обслуживание информационных систем*

- ***Менеджмент технических уязвимостей***

Управление техническими уязвимостями

- Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры по устранению связанного с ними риска;



Этап 9.

Управление инцидентами информационной безопасности

2-ая ступень. Определение направления защиты

- *ЭТАП 9. Управление инцидентами информационной безопасности*

- ***Оповещение о нарушениях и недостатках информационной безопасности***

Оповещение о случаях нарушения информационной безопасности - О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно;

2-ая ступень. Определение направления защиты

- *ЭТАП 9. Управление инцидентами информационной безопасности*

- ***Оповещение о нарушениях и недостатках информационной безопасности***

Оповещение о недостатках безопасности - Все сотрудники, подрядчики и пользователи сторонних организаций, пользующиеся информационными системами и услугами, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в системах или услугах.

2-ая ступень. Определение направления защиты

- *ЭТАП 9. Управление инцидентами информационной безопасности*

- ***Управление инцидентами информационной безопасности и его усовершенствование***

Ответственность и процедуры - Должны быть установлены ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности;

2-ая ступень. Определение направления защиты

- *ЭТАП 9. Управление инцидентами информационной безопасности*

- ***Управление инцидентами информационной безопасности и его усовершенствование***

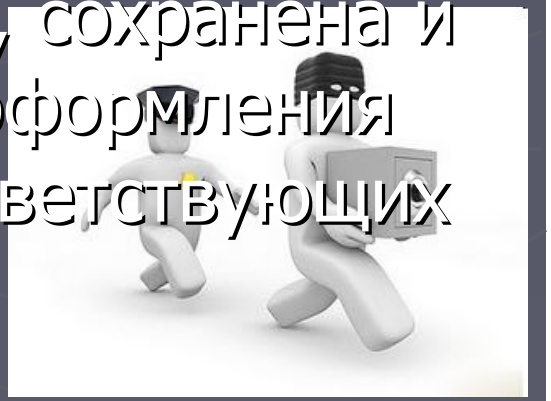
Извлечение уроков из инцидентов информационной безопасности - Должны быть определены механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям;

2-ая ступень. Определение направления защиты

- *ЭТАП 9. Управление инцидентами информационной безопасности*

- ***Управление инцидентами информационной безопасности и его усовершенствование***

Сбор доказательств - На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах.



Этап 10.

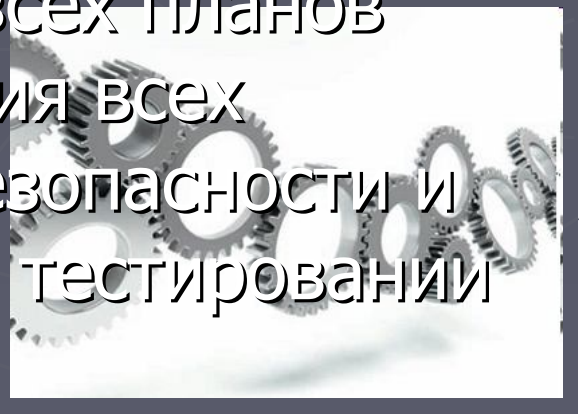
Управление непрерывностью бизнеса

2-ая ступень. Определение направления защиты

- *ЭТАП 10. Управление непрерывностью бизнеса*

- ***Вопросы информационной безопасности управления непрерывностью бизнеса***

Структура плана обеспечения непрерывности бизнеса - Должна быть создана единая структура планов непрерывности бизнеса, позволяющая обеспечить непротиворечивость всех планов для последовательного выполнения всех требований к информационной безопасности и для расстановки приоритетов при тестировании и обслуживании;



2-ая ступень. Определение направления защиты

- *ЭТАП 10. Управление непрерывностью бизнеса*

- ***Вопросы информационной безопасности управления непрерывностью бизнеса***

Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса - Планы по обеспечению непрерывности бизнеса должны подлежать регулярному пересмотру и обновлению с целью обеспечить их актуальность и эффективность;

Этап 11.

Соответствие требованиям

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Определение применимых норм - Все применимые нормы, установленные законодательством и исполнительными органами власти, требования договорных обязательств и порядок их выполнения следует четко определить, документировать и поддерживать на актуальном уровне для каждой информационной системы и организации;

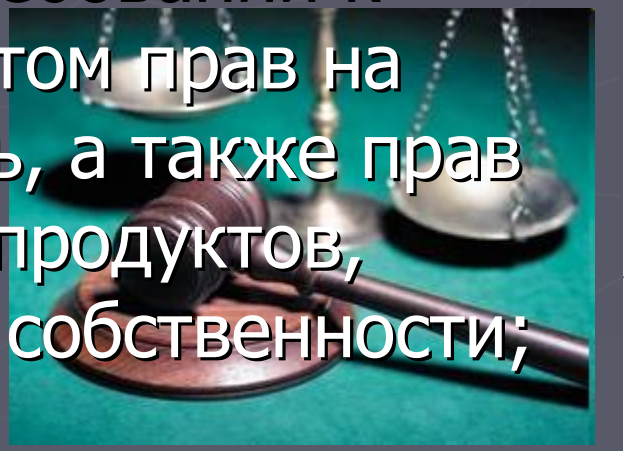
2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Права на интеллектуальную собственность

- Должны быть внедрены соответствующие процедуры для применения законодательных, регулирующих и контрактных требований к используемым материалам с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности;



2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Защита учетных записей организации - Важные учетные записи организации должны быть защищены от утраты, разрушения и фальсификации в соответствии с требованиями, установленными законами, документами органов исполнительной власти, контрактами и требованиями бизнеса;

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Защита данных и конфиденциальность персональной информации -Защита данных и конфиденциальность персональной информации должны быть обеспечены в соответствии с требованиями законов, нормативных актов и, где это применимо, в соответствии с положениями контрактов;

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Предотвращение нецелевого использования средств обработки информации - Должны быть применены меры контроля для предотвращения нецелевого использования средств обработки информации;

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*

- ***Соответствие правовым требованиям***

Регулирование использования средств криптографической защиты - Средства криптографической защиты должны быть использованы в соответствии с законами, нормативными актами и соответствующими соглашениями.

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*
- ***Вопросы аудита информационных систем***

Меры управления аудитом информационных систем - Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов;

2-ая ступень. Определение направления защиты

- *ЭТАП 11. Соответствие требованиям*
- ***Вопросы аудита информационных систем***

Защита инструментальных средств аудита информационных систем - Доступ к инструментальным средствам аудита информационных систем необходимо защищать для предотвращения любой возможности их неправильного использования или компрометации.

3-ая ступень. Техническая

- Нет единой методики или стандарта.
- По денежным средствам в организации, принимаются решения о покупке того или иного оборудования, ПО, систем.

3-ая ступень. Техническая

Что получим в итоге?

- ***Экономический эффект от вложений в ИБ!***

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 1 Осознание цели и выгоды внедрения СМИБ;
- 2 Получить поддержку руководства на внедрение СМИБ;
- 3 Создание рабочей группы по внедрению СМИБ (комиссия по защите информации в организации);
- 4 Обучение сотрудников отвечающих за внедрение СМИБ;

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 5 Проработать требования стандарта;
- 6 Сравнить требования стандарта с существующим положением дел;
- 7 Определить перечень мероприятий для достижения требований стандарта;
- 8 Разработать основной документ по защите информации (для оборонных – включить в Руководство по ПД ИТР (ссылка на ГОСТ), для коммерческих – в концепцию);

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 9 Разработать Концепцию ИБ;
- 10 Политика СМИБ;
- 11 Цели СМИБ;
- 12 Положение о применимости СМИБ;
- 13 Разработать «Политику ИБ» (ГОСТ Р ИСО/МЭК 17799—2005. Информационная технология. Практические правила управления информационной безопасностью), план обработки рисков;

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 14 Определить и утвердить направления, которые останутся в рисках (не подлежат контролю);
- 15 Определить необходимые новые документы для разработки;
- 16 Определить необходимые изменяемые документы;
- 17 Разработка новых документов;
- 18 Изменение существующих документов;

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 18 Изменение существующих документов;
- 19 Утверждение документов высшим руководством;
- 20 Обучение руководителей подразделений требованиям ИБ;
- 21 Обучение персонала требованиям ИБ;
- 22 Внедрение средств защиты (техническая часть);

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 23 Подбор команды внутреннего аудита по ИБ;
- 24 Планирование внутреннего аудита;
- 25 Проведение (выборочное) внутреннего аудита;
- 26 Проведение независимого внешнего аудита;
- 27 Проведение анализа СМИБ со стороны высшего руководства;

Алгоритм внедрения СМИБ в соответствии с требованиями международного стандарта ИСО 27001

- 28 Приказ высшего руководства о вводе в действие СМИБ;
- 29 Информирование клиентов, партнёров запуске СМИБ.

Чтобы не пустить деньги на ветер, необходимо помнить, что:

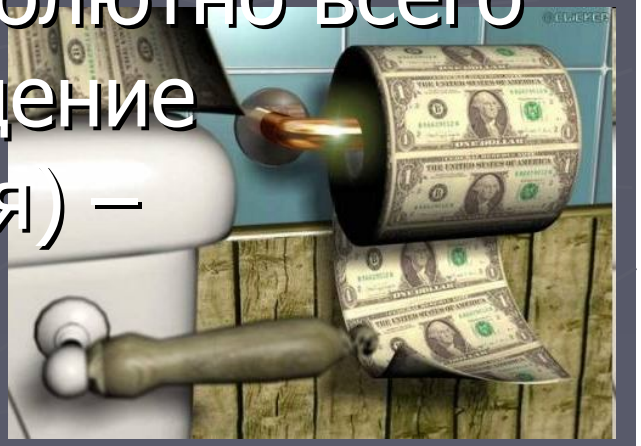
1 Необходимо наличие документированных контактов с различными инстанциями работающими в сфере информационной безопасности (ФСТЭК, ФСБ, форумы и выставки, обучение);

2 Периодически требуется проведение внешнего независимого аудита ИБ;

Чтобы не пустить деньги на ветер, необходимо помнить, что:

3 Постоянное ведение реестра информационных активов. *Работа колоссальная, но необходимая для обеспечения ИБ*;

4 Требования по ИБ должны применяться и выполняться при приёме абсолютно всего персонала на работу. Проведение анкетирования (тестирования) – обязательны!



Чтобы не пустить деньги на ветер, необходимо помнить, что:

5 Во время работы весь персонал периодически должен проходить обучение или инструктаж по информационной безопасности;

6 Должны быть разработаны и выполняться требования по ИБ для третьих лиц (дочерних компаний, провайдеров, арендаторов помещений);

Чтобы не пустить деньги на ветер, необходимо помнить, что:

7 Любое устройство, содержащее информацию, перед отправкой в ремонт, на склад, в утилизацию должно быть обработано на удаление конфиденциальной информации;

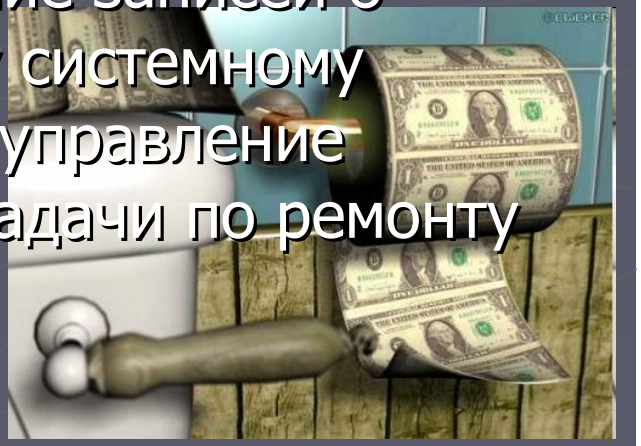
Чтобы не пустить деньги на ветер, необходимо помнить, что:

8 Системная документация ко всему оборудованию должна быть в наличии, доступна в любой момент времени и не должна быть доступна третьим лицам;

9 Необходимо учитывать требования ИБ не только к информационным системам, но и к другим каналам связи;

Чтобы не пустить деньги на ветер, необходимо помнить, что:

10 Все действия системных администраторов должны фиксироваться. Это особенно сложный пункт. Но его необходимость продиктована тем, что системные администраторы по роду своей деятельности постоянно корректируют (конфигурируют) настройки информационных систем. Уход с работы подобного сотрудника приведет к серьёзным финансовым последствиям для предприятия. Наличие записей о проделанных работах поможет новому системному администратору оперативно получить управление информационной системой и решать задачи по ремонту и наладке системы.



Чтобы не пустить деньги на ветер, необходимо помнить, что:

11 На всем предприятии должна применяться политика чистого рабочего стола (мебель) и экрана компьютера. Т.к. именно таким образом происходит большое количество утечек информации.

Чтобы не пустить деньги на ветер, необходимо помнить, что:

12 Все инциденты, другими словами все проблемы, связанные с информацией (поломка компьютера, кража оборудования, кража информации, сбой в работе информационной системы и др.) должны фиксироваться в едином реестре инцидентов;

13 На предприятии должны быть разработаны планы по восстановлению бизнеса. Камнем преткновения зачастую является их обязательное тестирование.

Спасибо, за внимание!

gordeevsa@teploobmennik.ru