# ПРОЦЕДУРНЫЙ УРОВЕНЬ ИБ

***Пестунова Тамара Михайловна***

*кандидат технических наук, доцент*

*проректор Новосибирского государственного университета экономики и управления*

*(383) 224-08-17*

*ptm@nsaem.ru*

# ЦЕЛИ И ЗАДАЧИ ПРОЦЕДУРНОГО УРОВНЯ ИБ

Процедурный уровень *включает в себя организационно-технические меры, направленные на людей.*

Цель мер процедурного уровня – *уменьшение рисков информационной безопасности, обусловленных «человеческим фактором».*

ВАЖНО:

*практика «докомпьютерного периода» не всегда соответствует современной ситуации,*

*Сейчас **основной акцент смещается на**:*

- *поддержание нормального функционирования аппаратного и программного обеспечения,*
- *внимание к вопросам доступности и целостности данных.*

# КЛАССЫ МЕР ПРОЦЕДУРНОГО УРОВНЯ

**Выделяются следующие группы мер процедурного уровня.**

- ***управление персоналом;***
- ***физическая защита;***
- ***поддержание работоспособности;***
- ***реагирование на нарушения режима безопасности;***
- ***планирование восстановительных работ.***

# ОБЩИЕ ПОДХОДЫ ПРИ УПРАВЛЕНИИ ПЕРСОНАЛОМ

**1. До приема на работу – описание должности.**

Цель: ***оценить ее критичность и спланировать процедуру проверки и отбора кандидатов.***

Два базовых принципа:

- Разделение обязанностей: ***один человек не может нарушить критически важный для организации процесс.***
- Минимизация привилегий: ***права доступа определяются служебных обязанностями.***

.

# ОБЩИЕ ПОДХОДЫ ПРИ УПРАВЛЕНИИ ПЕРСОНАЛОМ

**2. До заведения системного счета – обучение.**

- Служебные обязанности
- Нормы и процедуры информационной безопасности.

**3. В процессе работы – администрирование.**

Протоколирование и анализ действий пользователя;

Изменение профиля

**3. При увольнении - ликвидация системного счета.**

# ОБЩИЕ ПОДХОДЫ ПРИ УПРАВЛЕНИИ ПЕРСОНАЛОМ

**Администрирование лиц, работающих по контракту (выполнение внедренческих проектов, аутсорсинг и т.п.)**

Обратить внимание на

- ***Соблюдение принципа минимизации привилегий в процессе проекта*.**
- ***Корректность передачи функций администрирования «местным» сотрудникам в процессе внедрения***
- ***Проблемы удаленного администрирования (создаются дополнительные уязвимости)***

# ФИЗИЧЕСКАЯ ЗАЩИТА

**Включает:**

***защиту зданий и прилегающей территории,***
***поддерживающей инфраструктуры,***
***вычислительной техники,***
***носителей данных.***

**Основной принцип:**

***Непрерывность защиты в пространстве и времени***

# ФИЗИЧЕСКАЯ ЗАЩИТА

**Основные направления:**

- физическое управление доступом: ***контроль входа-выхода***

***Определить периметр безопасности и внешний интерфейс организации***

***Определить детальный порядок доступа на объекты внутри периметра***

***Применять автоматизированные средства контроля доступа***

- противопожарные меры

***противопожарной сигнализации***
***автоматические средства пожаротушения***

# ФИЗИЧЕСКАЯ ЗАЩИТА

- защита поддерживающей инфраструктуры –

***Защита систем электро-, водо- и теплоснабжения,***
***кондиционеров***
***средств коммуникаций***

Необходимо:

- ***защищать оборудование от краж и повреждений,***
- ***выбирать оборудование с максимальным временем наработки на отказ,***
- ***дублировать ответственные узлы,***
- ***иметь в резерве запчасти.***

# ФИЗИЧЕСКАЯ ЗАЩИТА

- защита от перехвата данных

***по оптическому,***
***вибро-акустическому***
***электромагинтному каналам,***

***с использованием мобильных носителей***

Меры: ***Расширение контролируемой зоны***
***Блокирование и зашумление***
***Использование криптографии***
***Управления подключением мобильных устройств.***

***Объем мер определяется значимостью аспекта конфиденциальности.***

- защита мобильных систем.

***Основная задача – не допустить кражи.***

# ОБЕСПЕЧЕНИЕ РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

**Основная проблема в большинстве случаев: - *Недооценка факторов безопасности в повседневной работе:***

- *Случайные ошибки системных администраторов и пользователей*
- *Наличие недокументированных систем*
- *Программные и программно-аппаратные конфликты (в том числе с системами безопасности)*

**Основные направления поддержания работоспособности ИС:**

- поддержка пользователей: ***консультирование и оказание помощи пользователям в решении возникающих проблем при работе с ИТ;***
- поддержка программного обеспечения

*контроль установки ПО*

*контроль отсутствия неавторизованных изменений* ***- в т.ч. поддержка эталонных копий систем, использование физических и логических средств управления доступом, применение утилит проверки целостности***

# ОБЕСПЕЧЕНИЕ РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

- конфигурационное управление – *обеспечить контроль и фиксирование изменений, вносимых в программную* конфигурацию;
- резервное копирование – *выработать регламент резервного копирования и обеспечить его соблюдение, хранить копии в безопасном месте, созавать несколько резервных копий, автоматизировать процесс, проверять периодически возможность восстановления;*
- управление носителями *обеспечивает конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем; обеспечить защиту носителей на физическом уровне.*
- Документирование – *документация должна быть актуальной и непротиворечивой, отражать текущее состояние дел.*
- регламентные работы – *могут создать серьезную угрозу, процесс должен быть жестко контролируем, работники – иметь высокую степень доверия.*

# РЕАГИРОВАНИЕ НА НАРУШЕНИЯ РЕЖИМА БЕЗОПАСНОСТИ

**Цели :**

- локализация инцидента и уменьшение наносимого вреда;
  ***«Горячая линия»*** *по вопросам реагирования, доступная круглосуточно*
  ***Оперативность реагирования*** *и скоординированность действий*
  ***Правильная расстановка приоритетов*** *(локализация инцидента и выявление нарушителя могут быть конфликтующими задачами)*
- выявление нарушителя;
  ***Взаимодействие с поставщиком сетевых услуг***
  ***Внутренние служебные расследования***
- предупреждение повторных нарушений.
  ***Анализ инцидентов, накопление статистики***
  ***Регулярный аудит и отслеживание новых уязвимостей***
  ***Корректировка программы безопасности***

# ПЛАНИРОВАНИЕ ВОССТАНОВИТЕЛЬНЫХ РАБОТ

**Планирование восстановительных работ позволяет**

*Быть в готовности на случай аварии,*

*Уменьшить ущерб от инцидентов*

*Сохранить способность к функционированию (возм.,в неполном объеме)*

**Основные этапы**:

- ***выявление критически важных функций*** *организации, установление приоритетов (полностью сохранить функционирование организации не всегда возможно);*
- ***идентификация ресурсов****, необходимых для выполнения критически важных функций в привязке к категориям:*

  ***персонал*** *(могут потребоваться специалисты разного профиля)* **,**

  ***информационная инфраструктура*** *(компьютеры; программы и данные, информационные сервисы внешних организаций, документация)*

  ***физическая инфраструктура*** *(здания, инженерные коммуникации, средства связи, оргтехника и др.);*

# ПЛАНИРОВАНИЕ ВОССТАНОВИТЕЛЬНЫХ РАБОТ

- ***определение перечня возможных аварий*** *(на основе сценариев вероятного развития событий);*
- ***разработка стратегии*** *восстановительных работ (базируется на наличных ресурсах и не должна быть слишком накладной для организации);*
- ***подготовка к реализации*** *выбранной стратегии;*
- ***проверка стратегии*** *проводится производится путем анализа подготовленного плана, принятых и намеченных мер*.

# ОСНОВНЫЕ АСПЕКТЫ ПРОГРАММНО-ТЕХНИЧЕСКОГО УРОВНЯ ИБ

**Программно-технический уровень** *включает меры, направленные на* ***контроль компьютерных сущностей - оборудования, программ и/или данных****.*

**Проблемы***: быстрое развитие ИТ предоставляет обороняющимся новые возможности и объективно затрудняет обеспечение надежной защиты только программно-техническими мерами.*

- **повышение быстродействия**, развитие параллелизма в вычислениях позволяет методом грубой силы преодолевать барьеры,
- **развитие сетевых технологий** расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- **появление новых информационных сервисов** обусловливает появление новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- **конкуренция среди производителей ПО** заставляет сокращать сроки разработки, что приводит к выпуску продуктов с дефектами защиты;
- **парадигма постоянного наращивания мощности** аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и вступает в конфликт с бюджетными ограничениями

# СЕРВИСЫ БЕЗОПАСНОСТИ

Относятся к категории вспомогательных сервисов. Включают:

- ***идентификация и аутентификация***;
- ***управление доступом***;
- ***протоколирование и аудит***;
- ***шифрование***;
- ***контроль целостности***;
- ***экранирование***;
- ***анализ защищенности***;
- **обеспечение *отказоустойчивости***;
- **обеспечение *безопасного восстановления***;
- ***туннелирование***;
- ***управление*.**

указанной совокупности, в целом, достаточно для построения надежной защиты на программно-техническом уровне. **НО**: необходимо соблюдение ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

# СЕРВИСЫ БЕЗОПАСНОСТИ

***Основные классы сервисов безопасности***

- ***превентивные, препятствующие нарушениям ИБ;***
- ***меры обнаружения нарушений;***
- ***локализующие, сужающие зону воздействия нарушений;***
- ***меры по выявлению нарушителя;***
- ***меры восстановления режима безопасности.***

# ОСОБЕННОСТИ СОВРЕМЕННЫХ КИС С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

- **Территориальная распределенность** *корпоративной сети с выходом за пределы контролируемой зоны, связи между сегментами находятся в ведении внешнего поставщика сетевых услуг.*
- **Наличие одного или несколько подключений к Internet**;
- **Территориальная распределенность важных серверов**, *доступ к которым нужен сотрудникам с разных площадок*, **мобильные пользователи** *и, возможно, сотрудники других организаций*;
- **Предоставление доступа не только с компьютеров**, *но и с использованием потребительских устройств (например, беспроводной связи);*
- **Работа пользователей с несколькими информационным сервисами в течение одного сеанса**, *опирающимся на разные аппаратно-программные платформы;*
- **Жесткие требования к доступности** *информационных сервисов (круглосуточное функционирования, минимизация времени простоя до нескольких минут);*

# ОСОБЕННОСТИ СОВРЕМЕННЫХ КИС С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

- **Присутствие активных агентов** *(например, апплеты), передаваемых с одной машины на другую и поддерживающих связь с удаленными компонентами;*
- **Не полный контроль пользовательских систем сетевыми и/или системными администраторами;**
- **Наличие ненадежного ПО** *(особенно полученное по сети), создающие проблемы в защите;*
- **Постоянное изменение конфигурации информационной системы** *на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.)*

**В целом, современные КИС – это *распределенные, разнородные, многосервисные, эволюционирующие системы.***

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ

*Теоретическая основа решения проблемы архитектурной безопасности – в интерпретации "Оранжевой книги" для сетевых конфигураций.*

"Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента.

Далее пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности.

Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации.

**Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации."**

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ

**Основные выводы из приведенного утверждения.**

- Необходимость выработки и проведения в жизнь единой политики безопасности;

- Необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;

- Необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал *полным набором защитных средств* и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ: ПРАКТИЧЕСКИЕ ПРИНЦИПЫ

- **непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;**
- **следование признанным стандартам, использование апробированных решений (*повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию* );**
- **иерархическая организация ИС с небольшим числом сущностей на каждом уровне (*обеспечивает управляемость системой*);**
- **усиление самого слабого звена;**
- **невозможность перехода в небезопасное состояние (*при любых обстоятельствах, в т.ч. нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ*);**

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ: ПРАКТИЧЕСКИЕ ПРИНЦИПЫ

- **минимизация привилегий** (***направлено на уменьшение ущерба от случайных или умышленных некорректных действий пользователей и администраторов***);
- **разделение обязанностей** (***один человек не должен иметь возможность нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников***);
- **эшелонированность обороны** (***нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался*** );
- **разнообразие защитных средств** (***усложняет для злоумышленника задачу проникновения в систему***);

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ: ПРАКТИЧЕСКИЕ ПРИНЦИПЫ

- **простота и управляемость информационной системы** (***Только для простого защитного средства можно формально или неформально доказать его корректность.***

  ***Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование*** )

# АРХИТЕКТУРНАЯ БЕЗОПАСНОСТЬ: ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

- **внесение в конфигурацию избыточности (*резервное оборудование, запасные каналы связи и т.п.*);**
- **наличие средств обнаружения нештатных ситуаций;**
- **наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность;**
- **рассредоточенность сетевого управления, отсутствие единой точки отказа;**
- **выделение подсетей и изоляция групп пользователей друг от друга (*ограничивает зону поражения при возможных нарушениях информационной безопасности*).**
- **минимизация объема защитных средств, выносимых на клиентские системы (*для доступа в корпоративную сеть могут использоваться потребительские устройства с ограниченной функциональностью; конфигурация клиентских систем может быть трудно контролируема* ).**