



«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. И.И. ПОЛЗУНОВА»
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автоматизированные системы управления

*Выполнила:
Студентка 2 курса ФИТ
Группы ИБ-71
Тарасова Анна*



Цель работы:

Ознакомиться с АСУ, с причинами их уязвимости и способами защиты, выполнить описание предметной области и анализ объекта исследования.

Задание к работе:

1. Изучить основные понятия.
2. Ознакомиться с АСУ, их структурой, видами, функциями и задачами.
3. Ознакомиться с причинами уязвимости АСУ и способами их защиты.
4. Описание предметной области и анализ объекта исследования.
5. Возможные проблемы и пути их решения.



«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. И.И. ПОЛЗУНОВА»
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автоматизированные системы управления

Автоматизированная система управления (АСУ) — комплекс аппаратных и программных средств, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия.





Цели АСУ

- предоставление лицу, принимающему решение (ЛПР), релевантных данных для принятия решений;
- ускорение выполнения отдельных операций по сбору и обработке данных;
- снижение количества решений, которые должно принимать ЛПР;
- повышение уровня контроля и исполнительской дисциплины;
- повышение оперативности управления;
- снижение затрат ЛПР на выполнение вспомогательных процессов;
- повышение степени обоснованности принимаемых решений.



Функции АСУ

Функции АСУ в общем случае включают в себя:

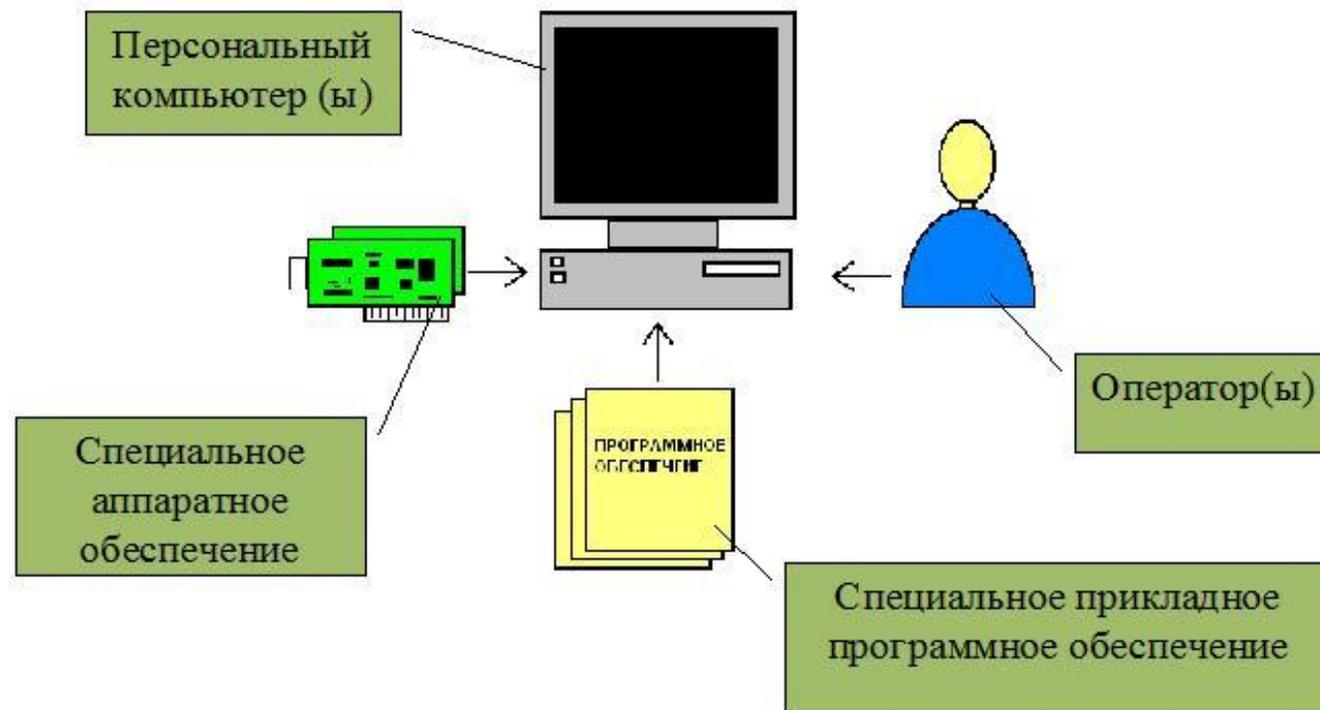
- планирование и прогнозирование;
- учет, контроль, анализ;
- координацию и регулирование.





Структура АСУ

Структурная схема автоматизированной системы управления





Виды АСУ

Автоматизированная система управления технологическим процессом или АСУ ТП — решает задачи оперативного управления и контроля техническими объектами в промышленности, энергетике, на транспорте.

«Система управления гостиницей».

Автоматизированная система управления производством (АСУ П) — решает задачи организации производства, включая основные производственные процессы, входящую и исходящую логистику.

«Автоматизированная система управления операционным риском» — это программное обеспечение, содержащее комплекс средств, необходимых для решения задач управления операционными рисками предприятий: от сбора данных до предоставления отчетности и построения прогнозов.



«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. И.И. ПОЛЗУНОВА»
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автоматизированная система управления иммунопрофилактикой

Автоматизированная система управления иммунопрофилактикой - программный комплекс «Управление иммунизацией» («Электронная картотека»), охватывающий все звенья управления и органически входящий в общую систему управления здравоохранением.

Комплекс состоит из набора программ, связанных единой информационной средой. В состав комплекса входят следующие подсистемы:

- комплекс программ управления иммунизацией в детской поликлинике;
- комплекс программ управления иммунизацией во взрослой поликлинике;
- комплекс программ сбора и обработки отчётно-аналитических документов (на уровне краевого центра медицинской профилактики);
- подсистема обмена информацией через телефонную сеть (электронная почта).



Разделы системы

Индивидуальное планирование и учет проведенных прививок детям и взрослым на уровне ЛПУ. Электронная обработка данных. Анализ реализации целевых показателей деятельности и передача результатов в администрации городов и районов края.

Анализ реализации целевых показателей деятельности администрациями городов и районов края с учетом деятельности ЛПУ и реализации муниципальных целевых подпрограмм «Вакцинопрофилактика». Передача результатов.

Анализ реализации планов профилактических прививок, привитости, расходованию МИБП, целевых показателей деятельности ЛПУ и администрации городов и районов края главным управлением Алтайского края по здравоохранению и фармацевтической деятельности. Передача результатов.

Принятие управленческих решений в отношении администраций городов и районов края управлением экономики и инвестиций администрации и главным управлением Алтайского края по здравоохранению и фармацевтической деятельности.



Причины уязвимостей АСУ ТП

Внешние факторы:

Системы промышленной автоматизации устарели и не учитывают современные киберугрозы;
Угрозы развиваются быстрее, чем защита. Уязвимости компонент систем управления не устраняются годами;
«Героизация» хакеров, высокий уровень грамотности и знаний у потенциальных взломщиков;
Доступность описания протоколов в открытых источниках.

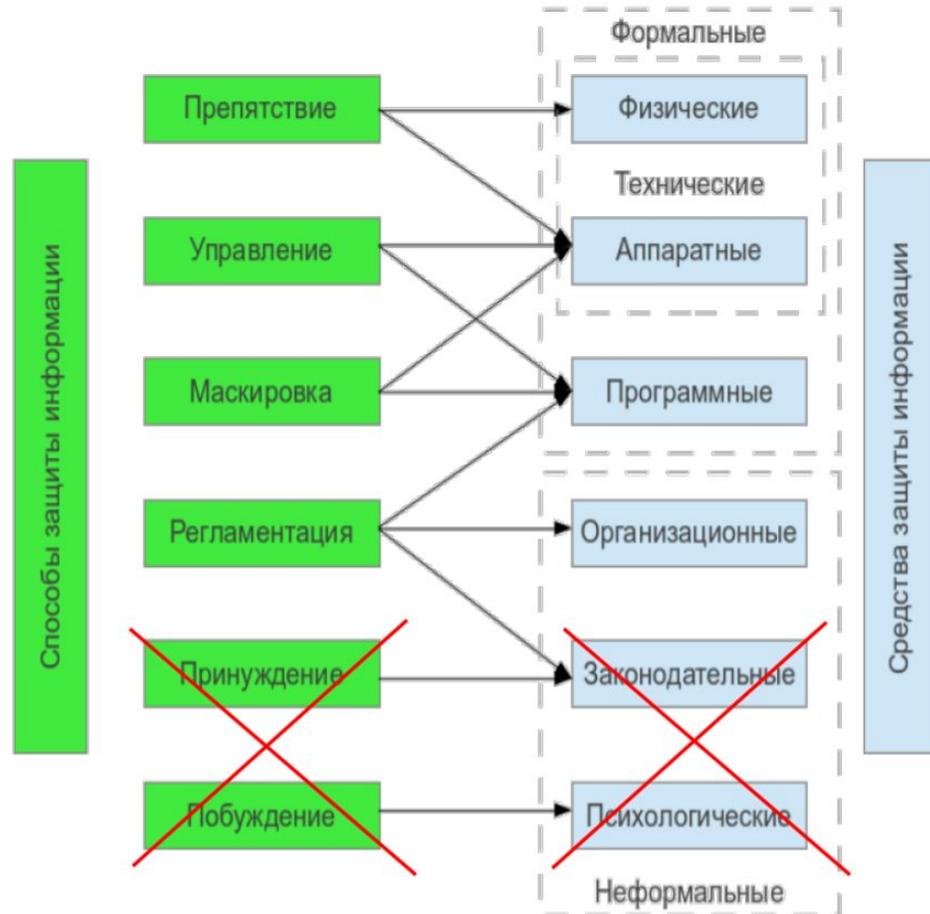


Внутренние факторы:

- Низкая грамотность технологов на предприятиях в области ИБ;
- Отсутствие правил информационной безопасности и регламентных мероприятий, связанных с работой на АСУ ТП;
- Влияние человеческого фактора (ошибки и неосмотрительность сотрудников, злой умысел бывших сотрудников).



Способы защиты



В рамках подхода к обеспечению информационной безопасности АСУ ТП не рассматриваются: административные способы защиты (принуждение и побуждение), связанные физические и неформальные средства защиты.



«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. И.И. ПОЛЗУНОВА»
 ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
 КАФЕДРА ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Технологии защиты

Способ защиты	Тип средства защиты	Средство защиты	Необходимость для защиты низких уровней АСУ ТП
Препятствие	Аппаратные, программные	Межсетевые экраны	Да
		Системы обнаружения и предотвращения вторжений	Да
		DLP-системы	Нет
Управление	Программные	Антивирус	Нет
		Средства анализа защищенности	Да
		Средства анализа кода	Да
		Средства контроля подключения съемных носителей	Нет
Маскировка	Аппаратные, программные	Средства доверенной нагрузки	Нет
		Средства криптографической защиты	Да
		Средства аутентификации и авторизации	Да



Схема работы АСУ иммунизацией



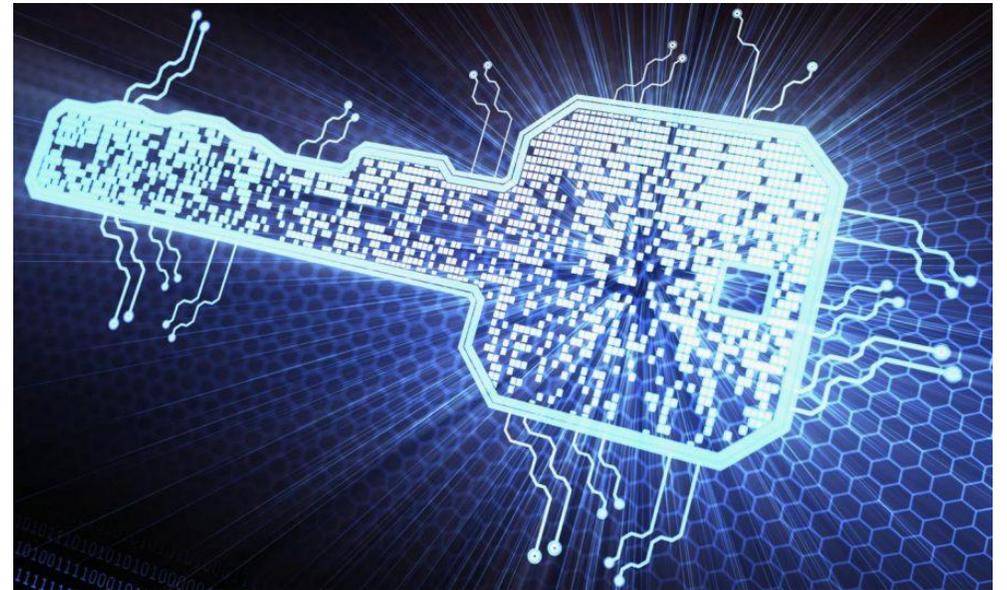
МИС – региональная медицинская информационная система (АРМ «Поликлиника»).



Возможные проблемы и пути их решения

Умышленные (преднамеренные) угрозы, обусловленные несанкционированными действиями обслуживающего персонала и несанкционированным доступом к ресурсам, в том числе и посторонними лицами.

Решения: средства контроля включения питания и загрузки программного обеспечения в ЭВМ, реализуемые на базе механических и электронных ключей, а также средства парольной защиты при "входе" в ЭВМ, как со стороны локальных, так и со стороны удаленных пользователей. В более общем случае можно рассматривать данный вид защиты как частный случай проблемы разграничения полномочий и доступа, и использовать соответствующие меры защиты.





Возможные проблемы и пути их решения

Неумышленные (непреднамеренные) угрозы, вызываемые ошибками в проектировании, в программном обеспечении, случайными сбоями в работе, энергоснабжения, ошибками пользователей и т.д.

Решение: при проектировании целесообразно рассмотреть вопросы противопожарной безопасности. Для зданий, расположенных в долинах рек или на побережье, весьма вероятной угрозой является затопление. В этих случаях средства целесообразно устанавливать на верхних этажах зданий и должны приниматься другие меры предосторожности. Нанесение ущерба ресурсам может также произойти в следствии стихийного бедствия. Ущерб может быть нанесен при технических авариях, например, при внезапном отключении электропитания и т.д.





Вывод:

В ходе данной работы были изучены основные понятия. Был выполнен анализ автоматизированной системы управления иммунизацией - программного комплекса «Управление иммунизацией» («Электронная картотека») в Алтайском крае.

Были найдены некоторые уязвимости в работе АСУ и предложены возможные пути их решения.

Цели и задачи, поставленные в начале работы, были достигнуты.