Министерство науки и высшего образования Российской Федерации

филиал федерального государственного автономного образовательного учреждения высшего образования

«Мурманский арктический университет»

(филиал МАУ в г. Кировске)

Форма обучения очная

Специальность 09.02.07

ОТЧЁТ

по практической работе

ПО МДК 05.01: Проектирование и дизайн информационных систем

Студента Волобуева И.Д. группы 2-ИСП-22-оКФ

Кировск

2024

ПРАКТИЧЕСКАЯ РАБОТА №10

Тема: Разработка требований безопасности ИС.

Цель работы: изучить требования, предъявляемые к защите информации, изучить документацию по защите информации; знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Наименование информационной системы: автоматизированная информационная система компании по обслуживанию вычислительной техники (АИС КОБВТ «Техноцентр»).

Назначение АИС КОБВТ «Техноцентр»: автоматизация управления процессом продажи, ремонта, сборки, тестирования компьютерной техники.

Компьютерная компания занимается продажей, ремонтом, сборкой, тестированием компьютерной техники. Также, специалисты компании предоставляют услуги по разработке и монтажу локальных вычислительных сетей. Вся техника и комплектующие закупаются оптом у дилеров и хранятся на складе. Клиент, который хочет приобрести товар, оформляет заказ в торговом зале, а забирает технику со склада или оставляет заявку на её доставку. Клиент, который хочет отремонтировать технику, приносит её в сервисный отдел, откуда, по прошествии некоторого времени, забирает как отремонтированную или как технику, не подлежащую ремонту. По желанию клиента, специалисты компании могут выехать к клиенту для общей диагностики возникшей проблемы с техникой. По результатам своей деятельности компьютерная компания производит отчисления в налоговые органы и предоставляет отчетность в органы государственной статистики.

1. Цель системы информационной безопасности (ИБ) у страховой медицинской компании заключается в обеспечении защиты конфиденциальности, целостности и доступности информации клиентов и компании.
2. Задачи системы ИБ.

– Предотвратить утечку конфиденциальных данных (медицинских данных клиента, личных документов клиента).

– Постараться минимизировать потери из-за природных катаклизмов.

1. Объекты системы ИБ.

* Данные о персонале – контактные данные, должности, права и т.д.
* Финансовая информация – какой доход/расход у компании, финансовые операции клиентов.
* Системы управления – сервера, база данных, сетевое оборудование и т.д.
* Сетевая инфраструктура – сети и коммуникационное оборудование.

1. Вероятные нарушители.

– Хакеры (своя выгода или просьба кого-то).

– Конкуренты (желают получить какую-то информацию или убрать с рынка соперника).

– Недобросовестные сотрудники или партнеры (хотят получить какую-то выгоду).

– Вредоносные программы (специально созданные для уничтожения системы компании или приобретённые из-за скаченного файла с неизвестного источника)

1. Основные виды угроз ИБ.

– Физический ущерб (пожар из-за нарушения ТБ, прорванные трубы, сломанные кондиционеры в специальном серверном помещение).

– Природные явления (сход лавин, землетрясения).

– Техногенные явления (пожар, аварии на атомной электростанции, терроризм, военные беспилотники).

– Несанкционированные действия (использование оборудования, копирование ПО, замена/удаления документов).

– Утрата важных серверов (нарушение энергоснабжения, отказ телекоммуникационного оборудования)

1. Классификация угроз.

– Преднамеренные (превышение полномочий сотрудников, внешние и внутренний атаки конкурентов/хакеров).

– Непреднамеренные (ошибочные действия сотрудника, сбой в работе ПО, недочеты системы защиты).

1. Политика паролей.

Метод установления подлинности происходит с помощью простого пароля (который содержит минимум 6 символов, в которые входят: цифры, минимум 1 строчная и 1 заглавная буква) и задержка времени (интервал времени между попытками регистрации или аутентификации начинает увеличиваться, начиная от трёх неудачных попыток).

Этот процесс установления подлинности с помощью простого пароля + задержка времени показано в рисунке 1:

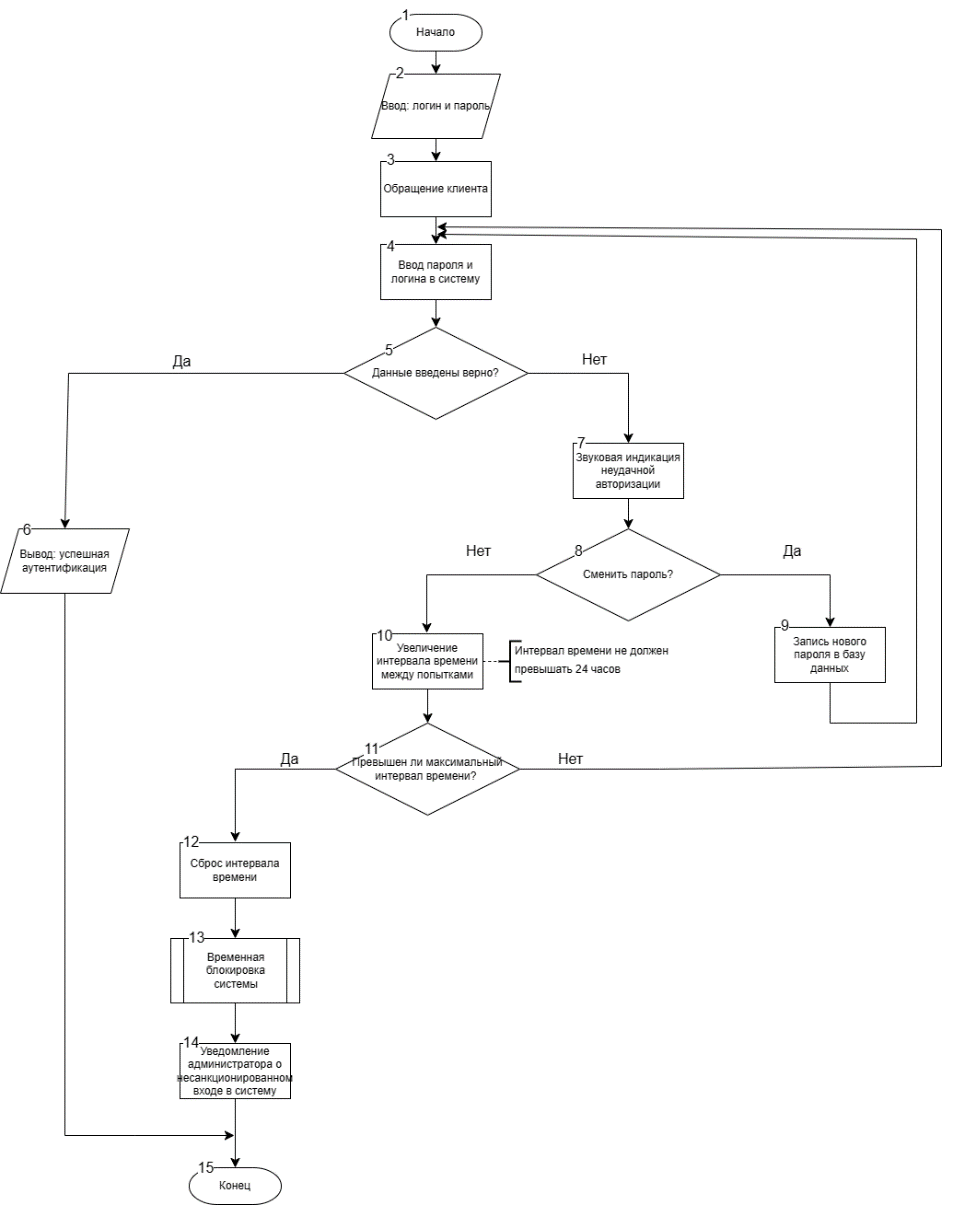


Рисунок 1 – Блок-схема для политике паролей

Раскрытие блока предопределенного процесса про временную блокировку системы показала в рисунке 2:

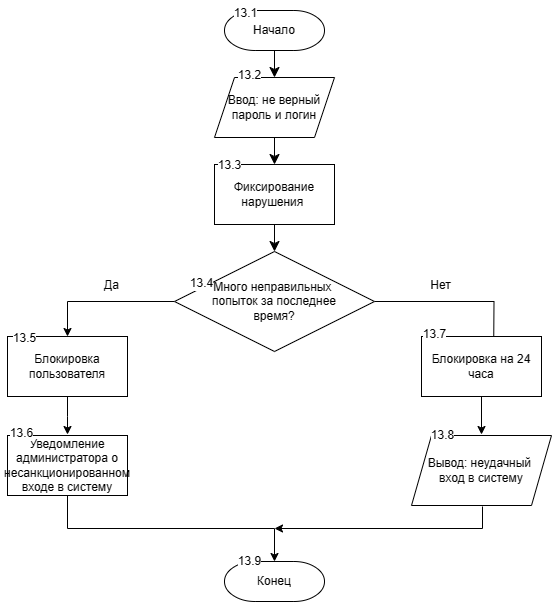


Рисунок 2 – Блок-схема временная блокировка системы