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 Лескив А.С. группы 2-ИСП-22-оКФ

Кировск  
2024

ПРАКТИЧЕСКАЯ РАБОТА №10

Тема: Разработка требований безопасности информационной системы.

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

1. Цель системы информационной безопасности для КОБВТ «Техноцентр» заключается в том, чтобы обеспечить:

* конфиденциальность информации клиентов и компании;
* целостность данных компании;
* доступность данных и систем;
* защиту от вредоносных программ и кибератак;
* мониторинг и анализ угроз;
* минимизация последствий аварий и стихийных бедствий.

1. Задачи системы информационной безопасности для КОБВТ «Техноцентр»:

* обеспечение конфиденциальности информации о клиентах, поставщиках и производственных процессов;
* защита от несанкционированного доступа к СУБД с данными о заказах и финансовыми учётами;
* защита от вредоносных программ и вирусов, которые могут нанести ущерб работе системы;
* обеспечение целостности данных клиентов и компании;
* мониторинг и обнаружение аномального поведения пользователей и утечек конфиденциальной информации;
* резервное копирование данных компании в случае катастрофы.

1. Объекты информационной безопасности для КОБВТ «Техноцентр»:

* система контроля доступа;
* антивирусное ПО;
* система мониторинга и аудита безопасности;
* система резервного копирования и восстановление данных;
* система обнаружения вторжений.

1. Вероятные нарушители ИБ для КОБВТ «Техноцентр»:

* внутренние угрозы (сотрудники, имеющие доступ к системе, могут случайно или намеренно нарушить безопасность);
* внешние угрозы (хакеры, которые могут попытаться нарушить безопасность системы или украсть данные);
* вирусы и вредоносное ПО (заражённые файлы);
* социальная инженерия (манипуляция сотрудниками для доступа данных или проникновение в систему).

1. Основные виды угроз ИБ (взяты из ГОСТ Р ИСО/МЭК 27005-2010, пункт 7.2 «Основные критерии»):

* физический ущерб (пожар, прорванные трубы, сломанные кондиционеры в серверной);
* природные явления (сход лавин);
* нарушения ИБ (например, утрата конфиденциальности, целостности и доступности);
* нарушения оперативной деятельности (как собственной, так и третьих сторон);
* потери ценности бизнеса и финансовой ценности;
* нарушения планов и конечных сроков;

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.

Вместо пароля для пользователей хранятся пары вопросов и ответов. Во время регистрации пользователь должен правильно ответить на вопрос, случайным образом выбранный из списка вопросов для данного пользователя. Система проверяет правильность введённого ответа. При неправильном вводе у пользователя есть 3 попытки. При их исчерпании происходит временная блокировка системы.

Этот процесс установления подлинности с помощью метода «Запрос-ответ» показано на рисунке 1.

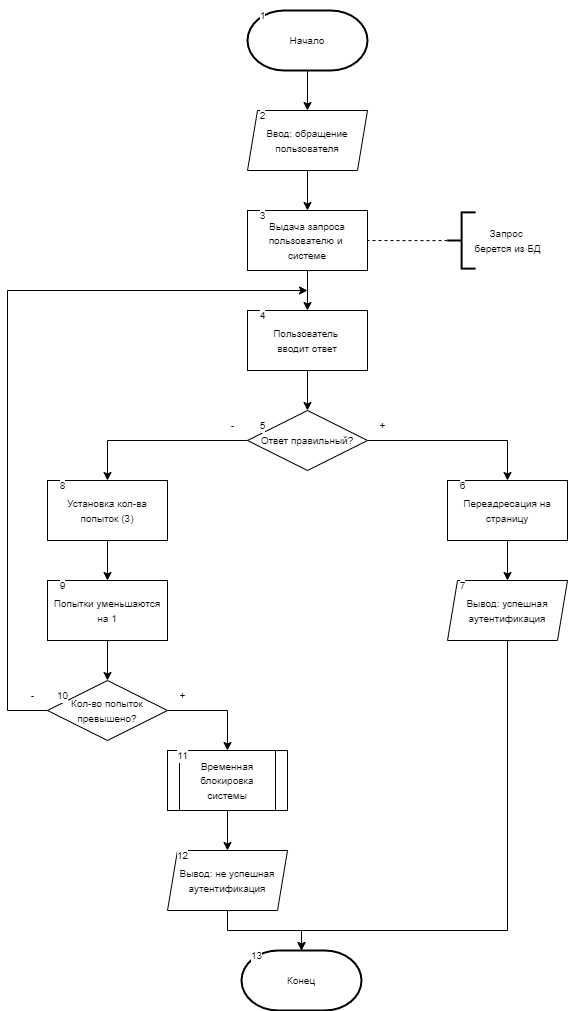


Рисунок 1 – Блок-схема политики паролей

Раскрытие блока №11 (временная блокировка системы) показано на рисунке 2.

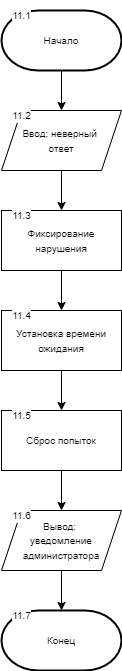


Рисунок 2 – Блок-схема временная блокировка системы