|  |  |  |
| --- | --- | --- |
| ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ» - ТОМСКИЙ ТЕХНИКУМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА | | |
| ПРОЕКТИРОВАНИЕ И ДИЗАЙН ИНФОРМАЦИОННЫХ СИСТЕМ | | |
| ОТЧЁТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ  «Разработка требований безопасности информационной системы» | | |
|  | | |
|  | Проверил: И.А. Абатуров | |
|  | Выполнил: Тесляк Игорь и Дружинин Семен | |
|  |  |  |
|  |  |  |
| 2023 | | |

**Задание №1**

**Цель:** обеспечение целостности, конфиденциальности и доступности защищаемой информации.

**Задачи:**

* Предупреждение, выявление и обнаружение угроз
* Локализация преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий
* Виды защищаемой на предприятии информации
* Степень её конфиденциальности
* Состав носителей защищаемой информации

**Задание №2**

* Влияние формы собственности на особенности защиты информации ограниченного доступа.
* Влияние организационно-правовой формы предприятия.
* Характер основной деятельности предприятия.
* Степень конфиденциальности защищаемой информации.
* Структура и территориальное расположение предприятия.

**Задание №3**

Возможности человека дестабилизировать ИС:

* Непосредственное воздействие на носители защищаемой информации
* Несанкционированное распространение конфидициальной информации
* Вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи
* Нарушение режима работы перечисленных средств и технологии обработки информации
* Вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

* Словесной передачи (сообщения) информации
* Передачи копий (снимков) носителей информации
* Показа носителей информации
* Ввода информации в вычислителные сети
* Опубликования информации в открытой печати
* Использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению
* Потеря носителей информации

Нейтрализация угроз осуществляется следующими методами:

* Блокировка ответа при неправильном числе запросов
* Искажение ответа путем округления и другой преднамеренной коррекции данных
* Разделение баз данных
* Случайный выбор записи для обработки
* Контекстно-ориентированная защита
* Контроль поступающих запросов

**Задание №4**

**Задание №5**

Требования к информационной безопасности:

* Проведение инструктажей
* Контроль съемных носителей
* Безопасность на уровне корпоративной сети компании
* Анализ рисков
* Система мониторинга ИБ-событий
* Обработка инцидентов ИБ
* Управление правами доступа
* Анализ антивирусной защиты
* Обеспечение эффективной и защищенной идентификации пользователей при получении доступа во внутренние системы компании

**Задание №6**

* Ограничить количество одновременно работающих пользователей в базе
* Скрыть «уникальные» алгоритмы или механизмы от потребителей или конкурентов
* Закрыть модули от заказчика до оплаты им разработанного модуля (конфигурации, подсистемы)
* Скрыть методы обмена с каким-то сервисом (веб-сервисом, сайтом и т.п.)
* Не допустить утечки разрабатываемой совместно конфигурации недобросовестными программистами-фрилансерами
* Установить пароль