|  |  |  |
| --- | --- | --- |
| 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: Полтораков Д.С. и Логинов А.А. | |
|  |  |  |
|  |  |  |
| 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**

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

**Задание №3**

Возможности человека дестабилизировать ИС:

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

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

1. Словесной передачи (сообщения) информации
2. Передачи копий (снимков) носителей информации
3. Показа носителей информации
4. Ввода информации в вычислителные сети
5. Опубликования информации в открытой печати
6. Использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению
7. Потеря носителей информации

Нейтрализация угроз осуществляется следующими методами:

1. Блокировка ответа при неправильном числе запросов
2. Искажение ответа путем округления и другой преднамеренной коррекции данных
3. Разделение баз данных
4. Случайный выбор записи для обработки
5. Контекстно-ориентированная защита
6. Контроль поступающих запросов

**Задание №4**

**Задание №5**

Требования к информационной безопасности:

1. Проведение инструктажей
2. Контроль съемных носителей
3. Безопасность на уровне корпоративной сети компании
4. Анализ рисков
5. Система мониторинга ИБ-событий
6. Обработка инцидентов ИБ
7. Управление правами доступа
8. Анализ антивирусной защиты
9. Обеспечение эффективной и защищенной идентификации пользователей при получении доступа во внутренние системы компании

**Задание №6**

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