|  |
| --- |
| Описание: Описание: для прик эмбл |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего профессионального образования"Российский технологический университет"МИРЭА |
| Институт «Комплексной безопасности и специального приборостроения» |
| Кафедра «Управление и моделирование систем» (КБ-3) |
|  |

|  |  |
| --- | --- |
| **Практика №1 по дисциплине** | |
|  | |
| **« Основы информационной безопасности »**  **«Политика безопасности»** | |
|  | |
| Выполнил студент группы БИСО-03-19 | *Ковалев П.А.* |

Москва 2020

ЗАДАНИЕ ПО СОСТАВЛЕНИЮ ПОЛИТИКИ ИБ

Логистическая компания ООО “Перевозчик” имеет штат в количестве 80 человек:

* управление компании (5 человек),
* курьеры (30 человек),
* бухгалтерия (10 человек),
* IT отдел (10 человек),
* отдел информационной безопасности (5 человек),
* охрана (4 человека),
* отдел по работе с клиентом (16)

Для общения между собой отделы используют общий чат в мессенджере или телефонную связь.

Управление компании имеет доступ ко всем программам, используемым в организации. Каждый следующий описанный отдел использует доступное для них ПО в формате «Чтение и запись (Read & Write)».

Курьеры для общения с клиентом используют специальный чат в приложении “Перевозчик”. Там же отмечают был ли выполнен или не выполнен заказ. Информация из приложения попадает в таблицу excel предприятия.

Отдел бухгалтерии использует приложения 1С Бухгалтерии и MS Office.

Отдел IT имеет доступ ко всем внутренним сетям предприятия, обеспечивает функционирование внутренней сети организации, а

также сайта компании и личных кабинетов клиентов и сотрудников. Для этого используется различные языки программирования, базы данных и приложения MS Office.

Отдел безопасности имеет такие же права, что и отдел IT, но также имеет доступ к проведению различных тестирований системы на наличии уязвимостей.

Охрана в своей работе использует общий чат в мессенджере и телефонную связь, а также имеют доступ к данным сотрудников.

Отдел по работе с клиентом ведет общение с клиентом по телефону или через чат на сайте предприятия. Отдел имеет доступ к информации, размещенной в программе MS Office.

Каждый сотрудник несет полную ответственность за свои действия во время работы на предприятии. В случае нарушения установленных норм сотрудника ждет наказание, зависящее от степени нарушения должностных обязанностей.

**Технический регламент для отдела информационной безопасности**

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных; (нужна модель угроз)

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных; (организационные меры по большей части и есть наши документы, плюс здесь нас отправляют читать дальше подзаконные акты)

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных; (очевидно нужен некий журнал учета и разработанные правила учета машинных носителей)

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер; (необходимо разработать некие правила обнаружения инцидентов и устранения их последствий, возможно, необходимо назначить группу реагирования на инциденты)

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; (нужны правила резервирования и восстановления)

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; (разработка системы допуска к данным, можно сделать на основе ролей в системе, так же само программное обеспечение должно уметь вести логи кто когда и к каким данным обращался)

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных. (нужен некий план периодического контроля, плюс, наверное, журнал, в котором будут фиксироваться результаты такого контроля)