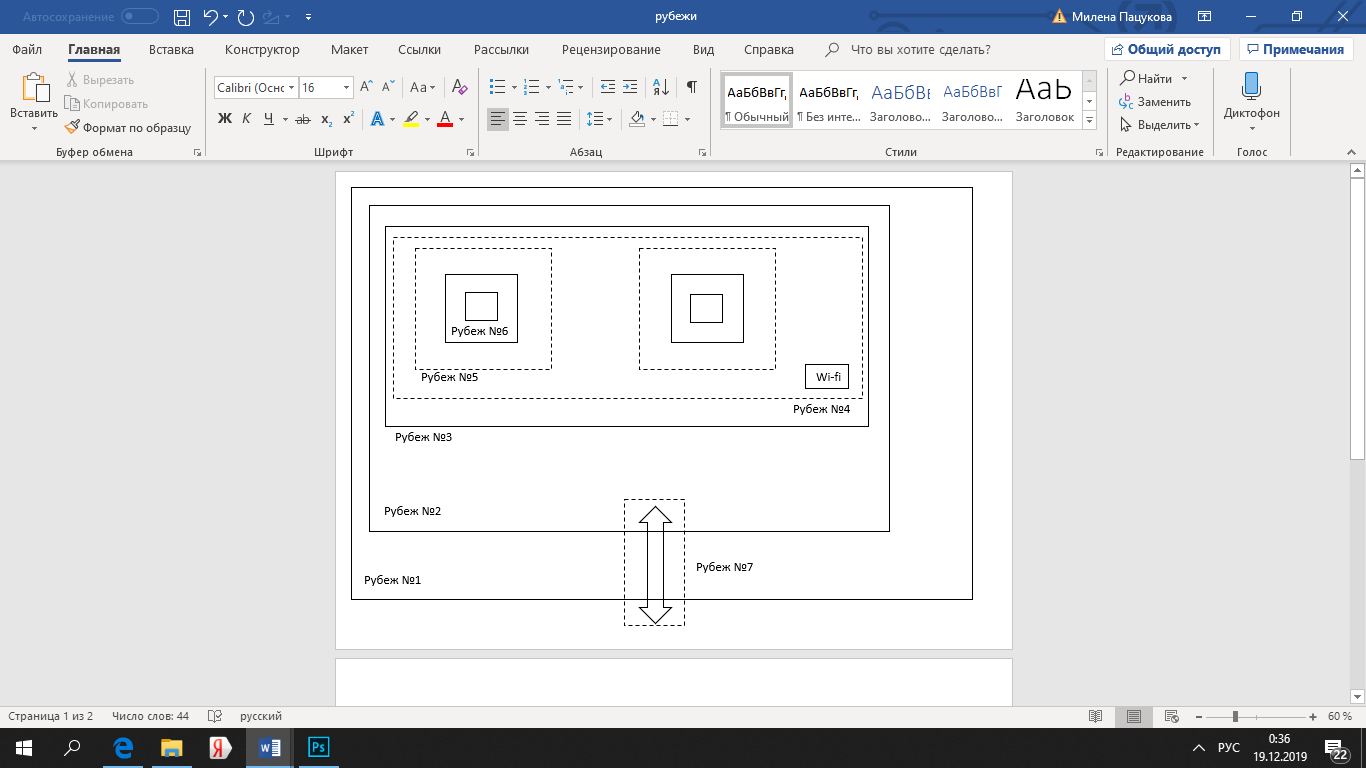
**Магазин одежды**

Пункт продажи и выдачи товаров, привозимых поставщиками. Пункт является франшизой.

**Категории информации:** ОД – ограниченный доступ, К – конфиденциальная информация, ИС – интеллектуальная собственность.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Рубеж защиты | Категория информации | Вид носителя/ вид информации | Вид НСД | Вид метода ЗИ |
| 1 | I | ОД | Ф/Ф, Эл/Эл | Ф | Ф |
| 2 | II | ИС | Ф/Ф, Эл/Эл | Ф | Ф |
| 3 | III | ИС | Ф/Ф | Ф | Ф |
| 4 | IV | ОД | Эл/Эл | ПА, А, П | ПА, А, П |
| 5 | V | К, ИС | Эл/Эл | П, А, ПА | П, А, ПА |
| 6 | VI | К | Эл/Эл | П | П |
| 7 | VII | ОД | Эл/Эл | П, А, ПА | П, А, ПА |

1. Территория бизнес-центра
2. Пропускной пункт в здание
3. Помещение магазина
4. Корпоративная сеть Wi-fi
5. Доступ к компьютеру
6. Учетная запись используемой программы
7. Сервер подключения к Интернет ресурсам

I рубеж – Территория бизнес-центра

II рубеж – Пропускной пункт в здание

III рубеж – Помещение магазина (ПО для оборудования магазина, являющееся интеллектуальной собственностью; документы на право владения предприятием; документы на право осуществления коммерческой деятельностью)

IV рубеж – Корпоративная сеть Wi-fi (сеть, связывающая помещение магазина, по ней передаются пд и данные финансового учета, а также различная служебная информация)

V рубеж – Доступ к компьютеру (специальное ПО для функционирования технического оборудования. ПО – является собственной интеллектуальной разработкой предприятия)

VI рубеж – Учетная запись используемой программы (специальное ПО для работы и обслуживания базы данных)

VII рубеж - Сервер подключения к Интернет ресурсам (сеть, связывающая корпоративную сеть с глобальным ресурсом сети Интернет)

|  |  |  |  |
| --- | --- | --- | --- |
| Рубеж | Физическое, техническое оснащение; | Виды угроз НСД | Методы защиты от угроз НСД |
| I | Забор, паркинг | * физические   + проникновение на территорию предприятия с целью совершения акта вандализма | * физические   + пропуск на вход осуществляется с 7:00 до 23:00 в соответствии с режимом объекта |
| II | Пост охраны | * физические   + пронесение третьим лицом шпионских устройств | * физические   + система входа по пропускам, при этом есть охранник, который сверяет лица входящих людей   + для посетителей ведётся учёт входа по паспорту, в систему вносятся его паспортные данные |
| III | Дверь с механическим замком | * физические   + получение информации путем прослушивания через открытую дверь, вентиляцию или стены   + получение информации через оптическое наблюдение   + физическое изъятие жесткого диска из системного блока ПК   + проникновение злоумышленника через дверь в ночное время * аппаратные   + получение информации путем установки скрытой видеокамеры или диктофона * программно-аппаратные   + скачивание третьими лицами конфиденциальной информации, относящейся к коммерческой тайне, или внедрение вредоносного ПО | * аппаратные   + установка доводчика двери, который плавно закрывает дверь после ее открытия   + установка локальных извещателей для охраны сейфа и ПК   + установка перед вентиляцией акустических экранов   + применение устройств для подавления сигналов скрыто работающего диктофона   + установка магнитно-контактного извещателя на дверь   + система сигнализации * физические   + применение тонированной пленки на стеклах, а также использование штор и жалюзи на окнах * программные   + противовирусное ПО для защиты информации   + доступ к файлам системы по PIN-коду с ограниченным числом попыток ввода |
| IV | wi-fi оборудование | * физические   + хищение информации сотрудником для передачи третьим лица или самим третьим лицом * программные   + перехват данных с помощью шпионских программ * аппаратные   + подключение к сети с помощью специальных устройств | * физические   + подписание договоров с сотрудниками о неразглашении коммерческой информации и персональных данных третьим лицам * программные   + использование VPN и межсетевого экранирования |
| V | Сеть ПК, главный компьютер | * физические   + передача информации о ПО оборудования третьим лицам   + скрытое наблюдение за процессом продажи через окна/двери с последующим возможным раскрытием конфиденциальной информации   + недобросовестное отношение к учёту продукции и поставкам * программно-аппаратные   + попытка взлома главного компьютера с помощью устройства подбора пароля   + попытки скачивания информации о ПО с целью последующей продажи * программные   + несанкционированный взлом системы и хищение данных   + установка вредоносного ПО для остановки работы специальных программ | * физические   + подписание контрактов с каждым из сотрудников о неразглашении коммерческой информации   + доступ к главному ПК имеет ограниченное число лиц * аппаратные   + доступ к главному компьютеру посредством ввода пароля   + дополнительные резервные места хранения информации * программные   + противовирусное ПО для защиты информации   + автоматическое копирование данных на резервные серверы   + доступ к файлам системы по паролю с ограниченным числом попыток ввода   + система распознавания несанкционированного взлома; самовыключение и связь с системой сигнализации |
| VI | Учетная персонализированная запись специальных программ | * физические   + передача информации о ПО оборудования третьим лицам   + скрытое наблюдение за процессом продажи через окна/двери с последующим возможным раскрытием конфиденциальной информации   + недобросовестное отношение к учёту продукции и поставкам * программно-аппаратные   + попытка взлома главного компьютера с помощью устройства подбора пароля   + попытки скачивания информации о ПО с целью последующей продажи * программные   + несанкционированный взлом системы и хищение данных   + установка вредоносного ПО для остановки работы специальных программ | * физические   + подписание контрактов с каждым из сотрудников о неразглашении коммерческой информации   + доступ к главному ПК имеет ограниченное число лиц * аппаратные   + доступ к главному компьютеру посредством ввода пароля   + дополнительные резервные места хранения информации * программные   + противовирусное ПО для защиты информации   + автоматическое копирование данных на резервные серверы   + доступ к файлам системы по паролю с ограниченным числом попыток ввода   + система распознавания несанкционированного взлома; самовыключение и связь с системой сигнализации |
| VII | Сервер подключения к Интернету | * Программные   + Утечка конфиденциальной информации в сеть Интернет   + Остановка работы по из-за сбоя сети   + Несанкционированный вход в систему и установление вредоносных программ с целью хищения/порчи данных * Аппаратные   + Установка устройства перехватывающего пакеты информации * Физические   + Повреждение кабеля передачи и связи с главным сервером | * Программные   + Установка противовирусного ПО   + Использование VPN   + Шифрование линий связи * Физические   + Профилактика на наличие вредоносных устройств |

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСиС»

Институт ИТАСУ

Кафедра АСУ

Курсовая работа

по дисциплине: «информационная безопасность и защита информации»

НА ТЕМУ: «1-3 рубежи ЗАЩИТЫ МАГАЗИНА ОДЕЖДЫ »

Выполнила: ст. гр. БПИ-17-1

Пацукова Милена

Проверила: доц. каф. АСУ

Бондаренко И. С.

Москва 2019 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСиС»

Институт ИТАСУ

Кафедра АСУ

Курсовая работа

по дисциплине: «информационная безопасность и защита информации»

НА ТЕМУ: «4-5 рубежи ЗАЩИТЫ МАГАЗИНА ОДЕЖДЫ »

Выполнил: ст. гр. БПИ-17-1

Назаренко Андрей

Проверила: доц. каф. АСУ

Бондаренко И. С.

Москва 2019 г.