**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное автономное**

**образовательное учреждение высшего образования**

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**ОТЧЁТ ПО УЧЕБНОЙ ПРАКТИКЕ**

**Тема: «Анализ требований к обеспечению защищённости операционных систем в зависимости от категории целевого объекта»**

**Выполнили:**

**ст. гр. 214-352, 241-353**

**Власова М. Н., Исламов Е. Р., Турбабин В.Д.**

**Проверили:**

**Кесель С. А.**

**Москва – 2025**

**Оглавление**

Задачи работы3

Введение4

Классификация целевых объектов и их особенности в контексте ИБ4

# Нормативные и методические документы по защите ОС5

Сравнение требований к защищённости ОС для разных объектов5

Анализ ОС на соответствие требованиям 6

Вывод 7

Список использованных источников7

# **Задачи работы**

# Изучить классификацию целевых объектов (АРМ, серверы, АСУ ТП, мобильные устройства и др.) и их особенности в контексте обеспечения ИБ.

# Изучить нормативные и методические документы (ФСТЭК, ФСБ, ГОСТ, профстандарты), регламентирующие требования к защите ОС.

# Сравнить требования к защищённости ОС для разных типов объектов: уровни доверия, разграничение доступа, контроль целостности, обновления.

# Проанализировать примеры ОС, применяемых в разных средах (например, Windows Server, Astra Linux, Android), и оценить их соответствие требованиям.

# **Введение**

В цифровом мире защита информации стала важной задачей для всех организаций, независимо от их размера. Операционные системы лежат в основе этой безопасности, и важно защищать их с учетом особенностей объектов, законов и текущих угроз.

# **Таблица 1. Классификация целевых объектов и их особенности в контексте ИБ**

|  |  |  |
| --- | --- | --- |
| **Тип объекта** | **Описание** | **Особенности защиты** |
| АРМ (рабочая станция) | Персональный компьютер пользователя, предназначенный для выполнения рабочих задач. | Защита от вредоносного ПО, контроль доступа, шифрование данных, регулярные обновления. |
| Серверы | Обеспечивают работу сетевых служб, хранение и обработку данных. | Высокие требования к разграничению доступа, мониторинг атак, резервирование, контроль целостности. |
| АСУ ТП (Автоматизированные системы управления технологическими процессами) | Управление промышленными объектами (энергетика, транспорт, производство). | Защита от кибератак, контроль физического доступа, минимальное использование сетевых функций. |
| Мобильные устройства | Смартфоны, планшеты, IoT-устройства. | Шифрование данных, защита от утечек, контроль установки приложений, удалённое управление. |

# **Таблица 2. Нормативные и методические документы по защите ОС**

|  |  |  |
| --- | --- | --- |
| **Документ** | **Орган** | **Основные требования** |
| Приказ ФСТЭК № 239 | ФСТЭК | Требования к защите информации в государственных информационных системах (ГИС). |
| ГОСТ Р 57580.1–2017 | Росстандарт | Базовые требования к средствам защиты информации. |
| Приказ ФСБ № 378 | ФСБ | Требования к криптографической защите информации. |
| Профстандарт "Специалист по ИБ" | Минтруд | Определяет компетенции специалистов по защите информации. |

**Таблица 3. Сравнение требований к защищённости ОС для разных объектов**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **АРМ** | **Серверы** | **АСУ ТП** | **Мобильные устройства** |
| Уровень доверия | Средний (3–4 УЗ) | Высокий (1–2 УЗ) | Критический (1 УЗ) | Низкий-Средний (4–5 УЗ) |
| Разграничение доступа | Ролевая модель (RBAC) | Мандатное управление (MAC) | Жёсткий контроль (MAC + DAC) | App Sandboxing, RBAC |
| Контроль целостности | Хеш-суммы, ЭЦП | Сигнатурный анализ, HIDS | Аппаратные модули доверия (TPM) | Проверка приложений (Google Play Protect) |
| Обновления | Автоматические | Тестируемые + ручное развёртывание | Запрещены в рабочем режиме | Автоматические с задержкой |

# **Таблица 4. Анализ ОС на соответствие требованиям**

|  |  |  |  |
| --- | --- | --- | --- |
| **ОС** | **Применение** | **Соответствие стандартам** | **Недостатки** |
| Windows 10/11 | АРМ, офисные системы | ФСТЭК (3–4 УЗ), ГОСТ Р 57580 | Уязвимости нулевого дня |
| Windows Server | Корпоративные серверы | ФСТЭК (2 УЗ), ФСБ (СКЗИ) | Требует доп. настройки для MAC |
| Astra Linux | Госсектор, АСУ ТП | ФСТЭК (1 УЗ), СЗИ в реестре | Ограниченная поддержка ПО |
| Android | Мобильные устройства | FIPS 140–2, Common Criteria | Фрагментация, уязвимости прошивок |
| QNX | |  |  | | --- | --- | | Промышленные системы |  | | IEC 62443, ГОСТ Р | Закрытость, дорогое сопровождение |

# **Пояснение:** Уязвимость нулевого дня (англ. *Zero-Day*) — это ошибка в программном обеспечении, о которой неизвестно разработчику, но которая уже может эксплуатироваться злоумышленниками. Название происходит от того, что у разработчика "0 дней" на исправление до момента атаки.

# **Вывод**

# В ходе работы изучены классификация целевых объектов, нормативные требования к защите ОС и проведён сравнительный анализ операционных систем. Наиболее защищёнными являются специализированные ОС (Astra Linux), тогда как массовые решения (Windows, Android) требуют дополнительной настройки для соответствия стандартам ИБ.

**5. Список использованных источников**

1. ISO/IEC 15408:2022 "Common Criteria for Information Technology Security Evaluation".
2. U.S. Department of Defense. "Trusted Computer System Evaluation Criteria (TCSEC)" // DoD 5200.28-STD, 1985.
3. ГОСТ Р 57580.1–2017 "Безопасность финансовых организаций. Базовый набор организационных и технических мер защиты информации".