**Практика 1**

**Цель работы**: получение навыков систематизации и описания объекта информатизации, подход к формированию перечня требований к информационной безопасности.

Задание выполняется **в группах**.

Подготовка материала для выполнения практических заданий: описание объекта информатизации для моделирования угроз и разработки организационных документов по информационной безопасности.

1. Описать область деятельности, составить примерный перечень лицензий организации
2. Составить список основных рабочих процессов (*также в относительно обобщенном виде, но с учетом результата каждого процесса и основных шагов*). Обратите внимание, что рабочие процессы составляются не от должностей, а именно от процессов деятельности организации / предприятия.
3. Составить список вспомогательных рабочих процессов (связанные с управлением персоналом, финансами и т.д.)
4. Определить в организации, исходя из преимущественной автоматизации и цифровизации процессов:
   1. Используемые ИС
   2. Используемые АСУ (АСУ ТП) (при наличии)
   3. Используемые ИТКС (при наличии)
   4. Прочие системы (при наличии)
5. Описать должности, число работников на должностях, примерные обязанности (в нескольких коротких пунктах). Только необходимые (*должностную инструкцию составлять не нужно, просто определить в самых общих чертах*).
6. Разработать схемы
   1. Помещения(ий) организации, включая внешние точки при необходимости, и отметить **рабочие места** сотрудников
   2. Для каждой системы из п.IV, составить отдельную схему расположения **АРМ, серверов, линий связи**.
   3. Составить общую схему ИТ организации на основе п.VI(b), проверить корректность
   4. Укажите рабочее место(а) осуществляющие взаимодействие с ГИС.
7. Составить список оборудования для каждой системы из п.IV, сверив со схемой п. VI, чтобы оборудование на ней фигурировало[[1]](#footnote-1) (*включая ИТ- оборудование*)
8. Составить список используемого ПО для каждой системы из п.IV (*на обобщенном уровне: ОС, Офисный пакет, Бухгалтерская программа и т.д*.) и составить таблицу кто с каким оборудованием и ПО работает, согласно должностям.
9. Для каждой ИСПДн организации указать:
   1. Базу данных (*включая ПО с помощью которого данные хранятся*) с перечнем обрабатываемых персональных данных и пометкой, являются ли это ПДн сотрудников организации;
   2. Средства обработки ПДн (*программное обеспечение; проверьте соответствие со списком выше*);
   3. Должности сотрудников, работающих с ИСПДн
   4. АРМ на которых обрабатываются ПДн (*проверьте соответствие со списком и схемой выше*)
   5. **Определить уровень защищенности каждой ИСПДН на основе ФЗ-152 и его подзаконных актов**.
10. Определить и обосновать отнесение организации к КИИ на основе ФЗ-187
11. Определите **перечень отраслевых документов** и перечней **типовых ОКИИ**, относящихся к организации. *При необходимости по результатам скорректируйте предыдущие пункты.*
12. Для каждой ИС/АСУ/ИТКС (см. п IV) на основе действующей редакции ПП-127 **предложите с обоснованием категорию значимости**.
13. При наличии в организации коммерческой тайны или другой конфиденциальной/защищаемой информации также ее выделить в отдельные перечни.

**Оформить результат в виде:**

1. Презентации для рассказа
2. Развернутого отчета в формате doc/docx/odt

**Вариант 2.**

1. **Область деятельности**: Производство дронов; Сборка автоматизирована, дроны гражданского и военного назначения. Разрабатываются собственные «прошивки» и модификации выпускаемой продукции, оказывается техническая поддержка пользователей сети Интернет.

Автоматизированное взаимодействие с налоговой службой и государственным оборонным заказчиком через их ГИС.

Лицензии:

* **Лицензия на производство и реализацию беспилотных летательных аппаратов:** в зависимости от типа дронов и их предназначения может потребоваться специальная лицензия на их производство и продажу.
* **Сертификация качества:** необходима для подтверждения соответствия производимых дронов установленным нормам и стандартам качества.
* **Разрешение на использование воздушного пространства:** если планируется коммерческое использование дронов, требуется получение разрешения на их эксплуатацию в воздушном пространстве.
* **Регистрация товарного знака или бренда:** для защиты интеллектуальной собственности и предотвращения возможного копирования продукции другими производителями.
* **Другие специальные лицензии и разрешения:** в зависимости от конкретной специфики деятельности могут потребоваться и другие специальные разрешения и лицензии.

**ОКВЭД**(Общероссийский классификатор видов экономической деятельности) играет ключевую роль при регистрации предприятия в сфере производства дронов, определяя основные направления деятельности компании и влияя на такие аспекты, как налогообложение и лицензирование.

**Для производства дронов подходят следующие основные ОКВЭДы:**

* **26.51**- производство электронных компонентов.
* **26.30**- производство электронных и оптических приборов, непригодных для производства в других отраслях.
* **30.30**- производство самолетов, вертолетов, планеров и прочих летательных аппаратов; производство космических аппаратов и других космических транспортных средств, а также их частей.
* **33.17**- ремонт и техническое обслуживание воздушных и космических средств, включая их двигатели.
* **71.12**- инженерная деятельность и связанные с ней технические консультации.
* **72.19**- научные исследования и разработки в области естественных и технических наук.
* **74.90**- прочие профессиональные, научные и технические деятельности, не включенные в другие группировки.
* **46.69**- оптовая торговля прочими машинами и оборудованием.
* **46.75**- оптовая торговля прочими строительными материалами и изделиями.
* **47.91**- розничная торговля, осуществляемая независимо от места продажи, прочими машинами и оборудованием.
* **47.99**- розничная торговля в специализированных магазинах прочими новыми товарами в свободной торговле.

1. **Основные процессы**
2. Исследование и разработка (RD)
   1. Анализ требований военных заказчиков.
   2. Исследование новых технологий и материалов.
3. Проектирование
   1. Создание концептуальных моделей.
   2. Разработка технических спецификаций.
   3. Инженерные расчеты и моделирование.
4. Разработка систем управления
   1. Проектирование и программирование бортовых систем.
   2. Создание систем навигации и связи.
5. Производство компонентов
   1. Изготовление и сборка аэродинамических элементов.
   2. Производство электронных компонентов и систем.
6. Сборка
   1. Сборка всех компонентов в единое целое.
   2. Интеграция систем управления и бортового оборудования.
7. Тестирование и валидация
   1. Проведение наземных и летных испытаний.
   2. Проверка на соответствие военным стандартам.
8. Логистика и снабжение
   1. Управление поставками материалов и комплектующих.
   2. Организация хранения и транспортировки готовой продукции.
9. Маркетинг и продажи
   1. Разработка стратегий продвижения продукции
   2. Участие в выставках и мероприятиях.
10. Обслуживание и поддержка клиентов
    1. Предоставление технической поддержки пользователям.
11. Управление безопасностью
    1. Обеспечение ИБ
12. **Вспомогательные процессы**
13. Ведение бухгалтерского учёта в компании
14. Работа с персоналом
15. Документация и сертификация:

• Подготовка необходимой документации для сертификации.

• Соблюдение нормативных требований.

1. Экологические процессы:

• Утилизация отходов производства.

• Снижение воздействия на окружающую среду.

1. **Автоматизация и цифровизация процессов:**
   * Используемые ИС

Техническая ИС: компьютеры, устройства для хранения/сбора/вывода и передачи данных, связные линии, оргтехника и документация ко всем.

Математическая и программная ИС: Программное обеспечение для точных расчетов, создания 3D моделей и чертежей, Программное обеспечение для создания электронных схем, Программы для системного администрирования, ОС, Компилятор языка программирования, Система версий проектов, дополнительно - IDE

* + Используемые АСУ (АСУ ТП)

Системы ЧПУ (Числового Программного Управления): системы от Siemens, Fanuc, Haas Automation. Эти системы управляют станками с ЧПУ, используемыми для обработки деталей дронов. SCADA-системы (Supervisory Control and Data Acquisition): Ignition, Wonderware InTouch, GE Proficy iFIX. Эти системы используются для мониторинга и управления производственными процессами в реальном времени, собирая данные с различных датчиков и устройств.

* + Используемые ИТКС

Серверное оборудование, системы бесперебойного питания и защиты данных (система управления доступом, фаеровол и тд), Система почты

* + Прочие системы

Система автоматизации логистики (например, 1С: Логистика), система автоматизации бухгалтерского учёта (например, 1С: Бухгалтерия), Таск-трекеры, Офисный пакет,

1. **Должности работников.**
2. **Инженер-конструктор**:

* Число работников: 5-10
* Обязанности:

Разработка конструкций дронов с учетом требований по аэродинамике, прочности и функциональности.

Создание 3D-моделей и чертежей.

Проведение расчетов для оценки характеристик летательных аппаратов.

Взаимодействие с другими отделами для интеграции различных систем.

ПО: ОС, Программное обеспечение для точных расчетов, создания 3D моделей и чертежей.

1. **Инженер-электронщик**

* Число работников: 5-10
* Обязанности:

Проектирование и разработка электронных систем управления дронами.

Разработка схем и печатных плат.

Тестирование и отладка электронных компонентов.

ПО: ОС, Программное обеспечение для создания электронных схем.

1. **Программист**

* Число работников: 3-7
* Обязанности:

Разработка программного обеспечения для управления дронами.

Написание кода для бортовых систем и наземных станций.

Обновление и поддержка программного обеспечения.

ПО: ОС, Компилятор языка программирования, Система версий проектов, дополнительно - IDE.

1. **Специалист по тестированию**

* Число работников: 3-5
* Обязанности:

Проведение испытаний дронов на различных этапах производства.

Анализ результатов тестирования и выявление недостатков.

Подготовка отчетов о тестировании.

ПО: ОС, Офисный пакет.

1. **Оператор производственной линии**

* Число работников: 10-20
* Обязанности:

Сборка компонентов дронов на автоматизированной линии.

Контроль качества сборки и соответствия стандартам.

Обслуживание и настройка оборудования.

ПО: ОС, Программное обеспечение для точных расчетов, офисный пакет

1. **Специалист по качеству**

* Число работников: 2-4
* Обязанности:

Контроль за соблюдением стандартов качества на всех этапах производства.

Проведение аудитов и инспекций.

Разработка и внедрение мероприятий по улучшению качества.

ПО: ОС, Офисный пакет.

1. **Логист**

* Число работников: 2-3
* Обязанности:

Организация поставок материалов и комплектующих для производства.

Управление запасами и складскими процессами.

Координация доставки готовой продукции

ПО: ОС, офисный пакет, система автоматизации логистики (например, 1С: Логистика)

1. **Менеджер проектов**

* Число работников: 1-2
* Обязанности:

Планирование и координация всех этапов разработки и производства дронов.

Управление бюджетом и сроками выполнения проектов.

Взаимодействие с заказчиками и заинтересованными сторонами.

ПО: ОС, офисный пакет, система ведения проектов (например, таск-трекеры)

1. **Специалист оп ремонту**

* Число работников: 3
* Обязанности:

Поддержка устройств клиентов, диагностика, ремонт

1. **Бухгалтер**

* Число работников: 1-2
* Обязанности:

Участие в разработке и дальнейших мероприятиях, направленных на рациональное и правильное использование ресурсов.

Прием и проведение контроля первичной документации.

Отражение на счетах операций, связанных с постоянным движением денежных и основных средств, ТМЦ.

Работа со бухгалтерской документацией (накладные, финансовые документы, договора).

Начисление заработной платы служащим предприятия.

ПО: ОС, Программное обеспечение для точных расчетов, офисный пакет, система автоматизации бухгалтерского учёта (например, 1С: Бухгалтерия)

1. **Системный администратор**

* Число работников: 1-2
* Обязанности:

Установка, настройка и обновление операционных систем, а также другого ПО и инфраструктуры.

Мониторинг и исправление ошибок в работе инфраструктуры разработки, ПО, сайта или приложения

Подготовка к возможной перегрузке или ошибке инфраструктуры

ПО: ОС, Программы для системного администрирования

1. **Офисные работники**

* Число работников: 5
* Обязанности:

Общение с клиентами

Работа с потенциальными клиентами, с заказчиками

Подготовка документации

ПО: ОС, офисный пакет.

1. **HR-специалист**

* Число работников: 1-2
* Обязанности:

Набор персонала

Работа с персоналом

1. **Специалист по экологии**

* Число работников: 1
* Обязанности:

Контроль за соблюдение экологических норм, подготовка соответствующих

1. **Специалист ИБ**

* Число работников: 1 -1

Обязанности:

* + Обеспечение ИБ на всех этапах разработки и обслуживания
  + Мониторинг угроз в реальном времени
  + Проведение профилактических бесед с сотрудниками

**IX**. **Для каждой ИСПДн**

**a. Базы данных:**

1. **1С Бухгалтерия**
   * **Назначение:** расчёт зарплаты, учёт кадров, налоговая отчётность.
   * **Состав ПДн:**
     + ФИО, паспортные данные, ИНН, СНИЛС, адреса сотрудников, банковские реквизиты, данные трудового договора, данные по заработной плате и отчислениям.
   * **ПДн сотрудников:** да.
   * **ПО для хранения:** 1С: Предприятие, MS SQL Server.
2. **Система учёта доступа**
   * **Назначение:** контроль и управление доступом к рабочим зонам и ИТ-системам.
   * **Состав ПДн:**
     + Логины пользователей, привилегии, журналы событий (дата/время входа, IP-адрес).
   * **ПДн сотрудников:** да.
   * **ПО для хранения:** система SIEM, базы на PostgreSQL.
3. **База данных клиентов (для гражданских дронов)**
   * **Назначение:** учёт заказов, обработка заявок клиентов.
   * **Состав ПДн:**
     + ФИО, контактные данные (телефон, email), адрес доставки, история заказов.
   * **ПДн сотрудников:** нет, только клиентов.
   * **ПО для хранения:** CRM-система.
4. **База данных контрактов (военные дроны)**
   * **Назначение:** хранение информации о заключённых контрактах.
   * **Состав ПДн:**
     + Контактные данные представителей заказчиков, паспортные данные для допуска.
   * **ПДн сотрудников:** нет.
   * **ПО для хранения:** специализированное ПО контрактного учёта (MS SQL Server).

**b. Средства обработки ПДн:**

**ПО:**

* + 1С: Предприятие для бухгалтерского учёта.
  + SIEM (система мониторинга и управления событиями безопасности).
  + PostgreSQL и MySQL для баз данных.
  + CRM-система для работы с клиентами.
  + Microsoft Office для обработки документации.

**Оборудование:**

* + Сервер хранения данных.
  + ПК сотрудников с доступом к ПО (установленные клиенты для 1С, CRM и SIEM).
  + Резервный сервер (для резервного копирования данных).

**c. Должности сотрудников, работающих с ИСПДн:**

1. **Бухгалтер:**
   * Обрабатывает ПДн сотрудников (1С: Предприятие).
2. **Администратор безопасности:**
   * Администрирует доступ к ИСПДн, ведёт журналы событий (SIEM).
3. **Менеджеры отдела продаж (для гражданских дронов):**
   * Работают с клиентской базой (CRM).

**d. АРМ для обработки ПДн:**

1. **АРМ бухгалтера:**
   * ПК с 1С: Предприятие, подключённый к серверу с базой данных.
2. **АРМ администратора безопасности:**
   * ПК с доступом к SIEM и серверу.
3. **АРМ менеджера проектов:**
   * Рабочие станции менеджера с доступом к CRM-системе.

**e. Уровень защищенности ИСПДн**

**Категории персональных данных**

* **1С Бухгалтерия**: Обрабатываются ПДн сотрудников, включая паспортные данные, ИНН, СНИЛС, банковские реквизиты, данные трудового договора, зарплата. **(Чувствительные данные)**
* **Система учёта доступа**: Логины, привилегии, журналы событий (дата/время входа, IP-адрес). **(Идентификаторы пользователей, но не чувствительные ПДн)**
* **База клиентов** (гражданские дроны): ФИО, контактные данные, адреса доставки. **(Обычные ПДн, без чувствительных данных)**
* **База контрактов** (военные дроны): Контактные данные заказчиков, паспортные данные для допуска. **(Чувствительные данные, так как есть паспортные данные)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ИСПДн** | **Количество субъектов ПДн** | **Значимость данных** | **Класс ИСПДн** |
| **1С Бухгалтерия** | Сотрудники компании (десятки-сотни) | Чувствительные ПДн | **2 класс** |
| **Система учёта доступа** | Сотрудники компании | Логины, журналы событий (критично для безопасности) | **3 класс** |
| **База клиентов** | Клиенты (много, но не чувствительные данные) | Обычные ПДн | **4 класс** |
| **База контрактов** | Ограниченный круг заказчиков | Паспортные данные | **3 класс** |

**1С Бухгалтерия → 2 уровень защиты**

**Система учёта доступа → 3 уровень защиты**

**База клиентов → 4 уровень защиты**

**База контрактов → 3 уровень защиты**

Для обеспечения защиты персональных данных в каждой системе необходимо:

* **Для 2-го уровня** (1С Бухгалтерия):
  + Антивирусная защита, шифрование данных, контроль доступа.
  + Регулярный аудит и мониторинг событий безопасности.
* **Для 3-го уровня** (Система учёта доступа, база контрактов):
  + Идентификация и аутентификация пользователей.
  + Контроль доступа, аудит действий администраторов.
* **Для 4-го уровня** (База клиентов):
  + Базовые меры защиты: антивирусы, резервное копирование, разграничение доступа.

**X**. **Отнесение организации к КИИ**

* 1. Основания для отнесения организации к КИИ

Согласно 187-ФЗ, объектами КИИ считаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления (АСУ), работа которых влияет на:

* Обороноспособность страны
* Безопасность государства
* Жизненно важные интересы личности, общества и государства

Для отнесения к КИИ организация должна относиться к одной из отраслей критической инфраструктуры, установленных в Постановлении Правительства РФ № 127 от 08.02.2018.

В данном случае предприятие занимается производством беспилотников, включая военные дроны. Это затрагивает оборонно-промышленный комплекс, который входит в перечень отраслей, связанных с КИИ.

2. Ключевые критерии отнесения к КИИ

2.1. Использование автоматизированных систем управления (АСУ ТП)

Организация использует АСУ ТП, в частности:

Системы ЧПУ (Siemens, Fanuc, Haas)

SCADA-системы (Ignition, Wonderware InTouch, iFIX)

АСУ ТП управляют производственными процессами, включая сборку и тестирование дронов. Нарушение их работы может привести к сбоям в производстве военной техники, что угрожает обороноспособности.

* 1. Информационные системы, взаимодействующие с государством

Компания использует автоматизированное взаимодействие с:

Налоговой службой

Государственным оборонным заказчиком через их ГИС

Это означает, что сбои в ее ИТ-инфраструктуре могут нарушить выполнение оборонных контрактов, что опять же затрагивает интересы государства.

* 1. Ключевые категории объектов КИИ

Согласно 187-ФЗ, объектами КИИ могут быть:

Автоматизированные системы управления (АСУ ТП) → у компании есть ЧПУ и SCADA.

Информационные системы госорганов → взаимодействие с оборонными структурами.

Информационные системы, обеспечивающие жизнедеятельность населения → производство дронов может затрагивать авиацию, логистику и безопасность.

1. Вывод

Данная организация подпадает под КИИ, поскольку:

✅ Входит в оборонно-промышленный комплекс (производит военные дроны).

✅ Имеет АСУ ТП, сбои в которых могут повлиять на производство.

✅ Взаимодействует с государственными системами (ГИС, налоговая).

Следовательно, в соответствии с ФЗ-187, организация должна зарегистрировать свои объекты КИИ, провести категорирование и обеспечить их защиту по требованиям ФСТЭК России.

**XI.** **Перечень отраслевых документов и перечней типовых ОКИИ, относящихся к организации**

Согласно ПП-127 и практике категорирования, к объектам КИИ организации могут быть отнесены:

* **АСУ ТП производственного процесса** (Системы ЧПУ, SCADA)
* **Информационные системы управления оборонными заказами**
* **Серверное и сетевое оборудование (ИТКС)**
* **Системы взаимодействия с налоговой и госзаказчиком**
* **Системы хранения и обработки данных по проектированию дронов**

**XII**. **Для каждой ИС/АСУ/ИТКС (см. п IV) на основе действующей редакции ПП-127 были определены категории значимости.**

В **ПП-127** прописано три категории значимости объектов КИИ:

* **I категория** — выход из строя повлияет на обороноспособность, экономическую или национальную безопасность.
* **II категория** — нарушение работы существенно влияет на отрасль (например, ОПК).
* **III категория** — нарушение влияет на отдельное предприятие, но не на всю отрасль.

1. **Категорирование систем в организации:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **ИС/АСУ/ИТКС** | **Описание** | **Категория значимости** | **Обоснование** |
| 1 | **АСУ ТП (ЧПУ, SCADA)** | Управляет производством дронов, в т.ч. военных. | **II категория** | Сбои приведут к срыву оборонных контрактов, но не критично для всей страны. |
| 2 | **ИС взаимодействия с госзаказчиком** | Связь с оборонными структурами, налоговой. | **II категория** | Нарушение работы вызовет сбои в военных поставках. |
| 3 | **ИТКС (серверы, СЗИ)** | Обеспечивает функционирование всех систем. | **II-III категория** | Атака может повлиять на работу предприятия, но не страны. |
| 4 | **ИС разработки ПО для дронов** | Хранение и разработка бортовых систем. | **II категория** | Компрометация приведет к утечке военных технологий. |
| 5 | **Система логистики (1С: Логистика)** | Управление поставками компонентов. | **III категория** | Сбой нарушит работу, но не критично для отрасли. |
| 6 | **Бухгалтерская система (1С: Бухгалтерия)** | Расчеты с сотрудниками, налогами. | **III категория** | Важна, но не критична для КИИ. |

**XIII**. **Наличие в организации коммерческой тайны или другой конфиденциальной/защищаемой информации**

* **1. Конфиденциальная информация (по 149-ФЗ)**
* Военные разработки (ПО, схемы, прошивки, 3D-модели)
* Данные о государственных заказах
* Технические характеристики дронов
* Данные сотрудников, включая персональные
* **2. Коммерческая тайна (по 98-ФЗ)**
* Финансовая отчетность, контракты с партнерами
* Сырье и комплектующие, поставщики
* Маркетинговые и стратегические планы
* Алгоритмы управления дронами

Для защиты этой информации должны применяться меры:

* Классификация информации и ограничение доступа
* Криптографическая защита (шифрование данных)
* Политики информационной безопасности (DLP-системы, контроль доступа)

1. Можно сделать несколько схем/ частей схемы чтобы избежать загромождения [↑](#footnote-ref-1)