1. Назначение системы

Класс Системы по проведению токовой диагностики электродвигателя по назначению – АСУ ТП.

По степени значимости – Класс 2 (Нару

-шение безопасности может привести к тяжким последствиям (крупные аварии, значительные финансовые потери, нарушение жизнедеятельности крупного населенного пункта).

1. Идентификация потенциальных угроз ИБ, определение вероятности реализации каждой из угроз ИБ проведены по результатам составления модели угроз безопасности информации при её обработке в автоматизированной системе по Методике оценки угроз безопасности информации, утверждённой ФСТЭК России в 2021 году (см. модель угроз).

|  |
| --- |
| УБИ.006 Угроза внедрения кода или данных |
| УБИ.008 Угроза восстановления аутентификационной информации |
| УБИ. 011 Угроза деавторизации санкционированного клиента беспроводной сети |
| УБИ.012 Угроза деструктивного изменения конфигурации/среды окружения программ |
| УБИ.013 Угроза деструктивного использования декларированного функционала BIOS |
| УБИ.014 Угроза длительного удержания вычислительных ресурсов пользователями |
| УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути |
| УБИ.017 Угроза доступа/перехвата/изменения HTTP cookies |
| УБИ.018 Угроза загрузки нештатной операционной системы |
| УБИ.019 Угроза заражения DNS-кеша |
| УБИ.022 Угроза избыточного выделения оперативной памяти |
| УБИ.023 Угроза изменения компонентов системы |
| УБИ.027 Угроза искажения вводимой и выводимой на периферийные устройства информации |
| УБИ.028 Угроза использования альтернативных путей доступа к ресурсам |
| УБИ.030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию |
| УБИ.031 Угроза использования механизмов авторизации для повышения привилегий |
| УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными |
| УБИ.041 Угроза межсайтового скриптинга |
| УБИ.049 Угроза нарушения целостности данных кеша |
| УБИ.059 Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов |
| УБИ.069 Угроза неправомерных действий в каналах связи |
| УБИ.071 Угроза несанкционированного восстановления удалённой защищаемой информации |
| УБИ.074 Угроза несанкционированного доступа к аутентификационной информации |
| УБИ.084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети |
| УБИ.086 Угроза несанкционированного изменения аутентификационной информации |
| УБИ.088 Угроза несанкционированного копирования защищаемой информации |
| УБИ.089 Угроза несанкционированного редактирования реестра |
| УБИ.090 Угроза несанкционированного создания учётной записи пользователя |
| УБИ.091 Угроза несанкционированного удаления защищаемой информации |
| УБИ.093 Угроза несанкционированного управления буфером |
| УБИ.098 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб |
| УБИ.099 Угроза обнаружения хостов |
| УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации |
| УБИ.103 Угроза определения типов объектов защиты |
| УБИ.104 Угроза определения топологии вычислительной сети |
| УБИ.115 Угроза перехвата вводимой и выводимой на периферийные устройства информации |
| УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети |
| УБИ.121 Угроза повреждения системного реестра |
| УБИ.123 Угроза подбора пароля BIOS |
| УБИ.128 Угроза подмены доверенного пользователя |
| УБИ.130 Угроза подмены содержимого сетевых ресурсов |
| УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании» |
| УБИ.152 Угроза удаления аутентификационной информации |
| УБИ.155 Угроза утраты вычислительных ресурсов |
| УБИ.158 Угроза форматирования носителей информации |
| УБИ.159 Угроза «форсированного веб-браузинга» |
| УБИ.162 Угроза эксплуатации цифровой подписи программного кода |
| УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов |
| УБИ.168 Угроза «кражи» учётной записи доступа к сетевым сервисам |
| УБИ.170 Угроза неправомерного шифрования информации |
| УБИ.171 Угроза скрытного включения вычислительного устройства в состав бот-сети |
| УБИ.172 Угроза распространения «почтовых червей» |
| УБИ.174 Угроза «фарминга» |
| УБИ.175 Угроза «фишинга» |
| УБИ.178 Угроза несанкционированного использования системных и сетевых утилит |
| УБИ.179 Угроза несанкционированной модификации защищаемой информации |
| УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации |
| УБИ.186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент |
| УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения |
| УБИ.192 Угроза использования уязвимых версий программного обеспечения |
| УБИ. 201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере |
| УБИ.208 Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники |
| УБИ.218 Угроза раскрытия информации о модели машинного обучения |
| УБИ.219 Угроза хищения обучающих данных |
| УБИ.220 Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта |
| УБИ.221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных |
| УБИ.222 Угроза подмены модели машинного обучения |
| УБИ. 223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии |
| УБИ. 224 Угроза нарушения целостности (подмены) контейнеров |
| УБИ. 225 Угроза нарушения изоляции контейнеров |
| УБИ. 226 Угроза внедрения вредоносного программного обеспечения в контейнеры |
| УБИ. 227 Угроза модификации (подмены) образов контейнеров |

1. Оценка вероятности наступления рисков, ущерб от реализации риска, актив, которому нанесён ущерб. Приоритизация рисков по уровню критичности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Риск ИБ** | **Вероятность исполения риска** | **Ущерб** | **Актив** |
| Риск перегрузки данных и атаки типа «отказ в обслуживании» (DDoS-атаки) (УБИ 140) | Высокая | Высокий | Доступность сервисов и систем. Атака может привести к временной недоступности сервисов, что нанесет ущерб работе компании. |
| Риск утечки конфиденциальной информации | Средняя | Высокий | Конфиденциальные данные компании. |
| Риск нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта (УБИ.220, внутренний + внешний нарушитель) | Высокая | Высокий | Рабочие алгоритмы и модели ИИ (если будет нарушена их корректная работа). Результаты анализа (ошибочные выводы могут повлиять на последующие действия компании или пользователей). |
| Риск потери аутентификационной информации | Средняя | Высокий | Конфиденциальные данные компании. Это может привести к утечке данных и нарушениям конфиденциальности. |
| Риск получения несанкционированного доступа к защищаемой информации | Средняя | Высокий | Конфиденциальные данные компании. Это может привести к утечке данных и нарушениям конфиденциальности. |
| Риск нарушения доступа к информации | Средняя | Высокий | Доступность данных и сервисов. Невозможность доступа к критически важным данным может парализовать бизнес-процессы. |
| Риск фишинговой атаки | Средняя | Высокий | Конфиденциальные данные компании. Это может привести к утечке данных и нарушениям конфиденциальности. |
| Риск нарушения целостности данных | Средняя | Высокий | Целостность данных компании. Искажение данных может привести к нарушению бизнес-процессов. |
| Риск компрометации данных из-за уязвимостей в ПО | Средняя | Высокий | Безопасность и целостность данных. Уязвимости могут быть использованы для внедрения вредоносного кода или утечки данных. |
| Риск компрометации данных через атаки на инфраструктуру машинного обучения | Средняя | Высокий | Результаты работы моделей машинного обучения. Атаки на инфраструктуру могут привести к неправильным решениям на основе некорректных данных. |
| Риск модификации модели машинного обучения путем искажения («отравления») обучающих данных | Средняя | Высокий | Точность модели машинного обучения. Отравленные данные могут снизить эффективность модели и привести к неверным выводам. |
| Риск подмены модели машинного обучения (УБИ.222, внутренний нарушитель) | Средняя | Высокий | Модель машинного обучения и результаты, основанные на её работе. Подмена модели может привести к неправильным решениям на основе некорректных данных. |
| Риск неправильной отработки модели машинного обучения | Средняя | Высокий | Модель машинного обучения и результаты, основанные на её работе. Неправильная отработка модели может привести к неправильным решениям на основе некорректных данных. |
| Риск хищения обучающих данных (УБИ.219, внутренний + внешний нарушитель) | Средняя | Высокий | Обучающие данные (наборы данных, используемые для обучения моделей ИИ).  Утечка конфиденциальной информации. |
| Риск несанкционированного удаления защищаемой информации | Низкая | Высокий | Критически важные данные компании. Могут быть затронуты целостность и доступность данных, что приведет к остановке бизнес-процессов. |
| Риск неконтролируемого распространения защищаемой информации | Низкая | Высокий | Конфиденциальные данные. Неконтролируемое распространение может нанести значительный ущерб компании. |
| Риск социальной инженерии | Высокая | Средний | Доступ к системам и данным. В результате социальной инженерии могут быть получены учетные данные сотрудников, что приведет к несанкционированному доступу. |
| Риск инверсионных атак на модель | Средняя | Средний | Модель машинного обучения. Инверсионные атаки могут раскрыть конфиденциальные данные, использованные при обучении модели. |

1. Анализ и примеры механизмов аудита и мониторинга аномалий, проработка схем реагирования на угрозы

Механизмы мониторинга и аудита аномалий ИБ:

1. SIEM-системы (Security Information and Event Management):

* Агрегация и корреляция событий с источников (логи, метрики).
* Правила и сценарии для выявления известных угроз (например, 10 неудачных входов подряд).

2. Системы обнаружения вторжений (IDS/IPS):

* Сетевые (NIDS): Анализ сетевого трафика на соответствие сигнатурам или аномалиям.
* Хостовые (HIDS): Мониторинг изменений на серверах (файлы, реестр).

3. UEBA (User and Entity Behavior Analytics):

* Машинное обучение для построения поведенческих профилей пользователей и сущностей.
* Обнаружение отклонений от базовой линии (например, вход в нерабочее время, доступ к необычным данным).

4. EDR (Endpoint Detection and Response):

* Мониторинг активности на конечных точках (рабочие станции, серверы).
* Анализ процессов, сетевых подключений и подозрительных действий в реальном времени.

5. Аудит логов (Log Management):

* Централизованный сбор и анализ логов критических систем (AD, VPN, БД, файерволы).
* Поиск по ключевым событиям и шаблонам.

6. Мониторинг целостности файлов (FIM):

* Контроль изменений критических файлов (исполняемые файлы, конфиги).

7. Анализ сетевого трафика (NTA/NDR):

* Выявление аномалий в сетевой активности (необычные объемы трафика, связи с подозрительными IP).

8. Дактилоскопия сетевых пакетов (DPI):

* Глубокий анализ для классификации трафика и выявления скрытых угроз.

9. Песочницы (Sandboxing):

* Исполнение подозрительных файлов в изолированной среде для выявления вредоносного поведения.

10. Контроль доступа и привилегий:

* Аудит использования учетных записей с повышенными правами.

1. Риски ИБ и мер их устранения

|  |  |  |  |
| --- | --- | --- | --- |
| Риск ИБ | Требования ИБ | СЗИ или орг. мера | Предложения по настройкам и размещению СЗИ |
| Риск утечки конфиденциальной информации | 1) Шифрование данных 2) Ролевая модель разграничения прав доступа | 1) Использование протокола TLS для передачи данных 2) Построение ролевой модели управления доступом. Системы контроля доступа привилегированных пользователей ( PAM ) 3) Регулярный аудит прав доступа | PAM |
| Риск несанкционированного удаления защищаемой информации | 1) Формирование многоуровневой защиты 2) Мониторинг активности пользователей | 1) Многоуровневая аутентификация 2) Внедрение SIEM-систем для мониторинга и анализа событий безопасности, регистрация и учёт событий в системе, в том числе событий безопасности, в объёме, достаточном для того, чтобы можно было отследить инцидента и расследовать их | Ankey SIEM NG («Газинформсервис») |
| Риск получения несанкционированного доступа к защищаемой информации | 1) Формирование многоуровневой защиты 2) Мониторинг активности пользователей 3) Разделение ландшафтов разработки, тестирования и эксплуатации и контроль доступа в них | 1) Многоуровневая аутентификация 2) Внедрение SIEM-систем для мониторинга и анализа событий безопасности, регистрация и учёт событий в системе, в том числе событий безопасности, в объёме, достаточном для того, чтобы можно было отследить инцидента и расследовать их 3) Межсетевое экранирование | Ankey SIEM NG («Газинформсервис»), Межсетевые экраны UserGate |
| Риск перегрузки данных и атаки типа «отказ в обслуживании» (DDoS-атаки) (УБИ 140) | Мониторинг активности и нагрузки на системы | 1) Настройка обеспечения качества обслуживания (QoS) 2) Внедрение систем обнаружения и предотвращения атак (IDS/IPS) | ViPNet IDS 3 (Инфотекс), «С-Терра СОВ» («С-Терра СиЭсПи») |
| Риск нарушения доступа к информации | 1) Отказоустойчивость IT-инфраструктуры 2) Резервное копирование 3) Разделение ландшафтов разработки, тестирования и эксплуатации и контроль доступа в них | 1) Балансировка нагрузки и поддержка непрерывности 2) Регулярное создание резервных копий 3) Межсетевое экранирование | 1) DNS-сервер 2) RuBackup  3) Межсетевые экраны UserGate |
| Риск нарушения целостности данных | Контроль версий и отслеживание изменений | 1) Использование хеширования для контроля целостности данных 2) Регулярные проверки целостности данных с использованием контрольных сумм |  |
| Риск компрометации данных из-за уязвимостей в ПО | 1) Регулярное обновление ПО  2) Проверка ПО на наличие уязвимостей | 1) Внедрение системы управления уязвимостями (Vulnerability Management System) | R‑Vision Vulnerability Management (VM) |
| Риск неконтролируемого распространения защищаемой информации | Контроль каналов передачи данных | 1) Внедрение политик DLP для контроля передачи данных 2) Внедрение шифрования электронной почты и других каналов передачи данных 3) Разработка инструкции пользователя корпоративной сети и обучение пользователей по информационной безопасности | SearchInform КИБ, InfoWatch Traffic Monitor |
| Риск социальной инженерии | Обучение персонала и повышение их осведомленности о методах социальной инженерии | 1) Назначение сотрудникам курсов по информационной безопасности 2) Фишинг рассылка для обучения сотрудников |  |
| Риск компрометации данных через атаки на инфраструктуру машинного обучения | 1) Защита инфраструктуры машинного обучения 2) Обеспечение безопасности серверов и среды выполнения моделей | 1) Использование методов защиты на уровне инфраструктуры, таких как сетевые экраны, системы обнаружения вторжений (IDS) и шифрование данных 2) Регулярное обновление серверов и систем хранения данных | ViPNet IDS 3 (Инфотекс), «С-Терра СОВ» («С-Терра СиЭсПи»), межсетевой экран UserGate |
| Риск инверсионных атак на модель | 1) Защита модели от утечек данных 2) Ограничение доступа к модели | 1) Регулярный аудит модели на предмет возможной утечки данных 2) Дифференциальная приватность |  |
| Риск модификации модели машинного обучения путем искажения («отравления») обучающих данных | 1) Обеспечение целостности и достоверности обучающих данных 2) Контроль доступа к данным | 1) Контролировать, чтобы входные данные из незначительного числа источников (например, от небольшой группы пользователей или IP-адресов) не составляли значительную часть обучающей выборки. Это может усложнить спамерам реализацию подобной атаки, поскольку им придется предпринимать дополнительные действия, чтобы их манипуляции не отбраковали как статистический выброс 2) Создать контрольный набор данных, для которых известен правильный результат оценки и на которых проверяется точность работы модели. 3) DevSecOps |  |
| Риск подмены модели машинного обучения (УБИ.222, внутренний нарушитель) | 1) Контроль доступа к данным 2) Логирование и мониторинг действий пользователей 3) Контроль версий моделей и кода 4) Шифрование и защита данных | 1) Настройка ролевой модели управления доступа. Системы контроля доступа привилегированных пользователей ( PAM ) 2) Внедрить SIEM систему для анализа логов и выявления аномалий. 3) Использовать инструменты DLP для предотвращения утечки данных. 4) Разработать и внедрить внутренние политики информационной безопасности, касающиеся управления и защиты моделей машинного обучения. 5) Проводить регулярные аудиты безопасности для проверки соответствия текущих практик установленным политикам и стандартам. 6) Аудит доступа сотрудников к данным 4) DevSecOps | Ankey SIEM NG («Газинформсервис»), SearchInform КИБ, InfoWatch Traffic Monitor, PAM, SAST, DAST |
| Риск хищения обучающих данных (УБИ.219, внутренний + внешний нарушитель) | 1) Контроль доступа к данным 2) Шифрование и защита данных 3) Логирование и мониторинг действий пользователей 4) Контроль копирования данных 5) Маскирование данных | 1) Настройка ролевой модели управления доступа. Системы контроля доступа привилегированных пользователей ( PAM ) 2) Использование протокола TLS для передачи данных 3) Внедрить SIEM систему для анализа логов и выявления аномалий. 4) Использовать инструменты DLP для предотвращения утечки данных. 5) Разработать и внедрить внутренние политики информационной безопасности, касающиеся управления и защиты моделей машинного обучения. 6) Проводить регулярные аудиты безопасности для проверки соответствия текущих практик установленным политикам и стандартам. 7) Аудит доступа сотрудников к данным 4) DevSecOps 5) SAST, DAST | Ankey SIEM NG («Газинформсервис»), SearchInform КИБ, InfoWatch Traffic Monitor, PAM, SAST, DAST |
| Риск нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта (УБИ.220, внутренний + внешний нарушитель) | 1) Контроль доступа к данным и многофакторная аутентификация 2) Шифрование и защита данных 3) Логирование и мониторинг действий пользователей | 1) Внедрить SIEM-систему для централизованного сбора и анализа логов с целью выявления и реагирования на инциденты безопасности. 2) Использовать системы IDS/IPS (Intrusion Detection/Prevention Systems) для обнаружения попыток несанкционированного доступа или модификации ИИ-систем. 3) Инструменты управления версиями и изменениями 4) Разделение среды разработки, тестирования и продакшн (обеспечить строгую сегментацию среды разработки, тестирования и продакшн, чтобы предотвратить внедрение неподтверждённых изменений в рабочую среду) 5) Разработать и внедрить внутренние политики информационной безопасности, касающиеся управления и защиты моделей машинного обучения. 6) Проводить регулярные аудиты безопасности для проверки соответствия текущих практик установленным политикам и стандартам. 7) Аудит доступа сотрудников к данным 4) DevSecOps | Ankey SIEM NG («Газинформсервис»),ViPNet IDS 3 (Инфотекс), «С-Терра СОВ» («С-Терра СиЭсПи»), Git (система управления версиями с распределенной архитектурой) |
| Риск фишинговой атаки | 1) Обучение персонала и повышение их осведомленности о методах фишинговых атак 2) Логирование и мониторинг действий пользователей 3) Контроль доступа к данным и многофакторная аутентификация | 1) Антивирусное ПО и шифрование данных. - Установка антивирусного ПО с функциями защиты электронной почты и веб-фильтрации.  - Шифрование данных при передаче и хранении для защиты от несанкционированного доступа. 2) Внедрение систем IDS/IPS для выявления и предотвращения попыток фишинговых атак. 3) Использование SIEM-систем для сбора, анализа и корреляции данных о событиях безопасности. 4) Использование решений для фильтрации спама и фишинговых сообщений (например, Secure Email Gateway).  5) Внедрение технологий анализа вложений и ссылок для выявления вредоносного контента. 6) Реализация многофакторной аутентификации для доступа к критически важным системам и данным. 7) Организация регулярного резервного копирования данных. 8) Разработка инструкции пользователя корпоративной сети и обучение пользователей по информационной безопасности | Kaspersky Security, ViPNet IDS 3 (Инфотекс), Ankey SIEM NG («Газинформсервис»), RuBackup |
| Риск потери аутентификационной информации | 1) Меры идентификации и аутентификации 2) Логирование и мониторинг действий пользователей 3) Управление доступом | 1) Доменные учетные записи, группы, уникальные идентификаторы пользователей ( логин, пароль, SSO), двухфакторная аутентификация (по СМС).  2) Централизованный контроль настроек ОС и компонентов  3) Ролевая модель управления доступом. Системы контроля доступа привилегированных пользователей ( PAM ) | MaxPatrol, Active Directory, IAM, PAM, SSO |
| Риск неправильной отработки модели машинного обучения | 1)Контроль версий модели и кода 2)Оценка предвзятости модели 3)Обфускация (запутывание) данных 4)Валидация данных 5)Охрана исходного кода модели 6)Мониторинг модели в процессе обучения | 1) Разработка и внедрение внутренних политик, касающихся обработки и обфускации данных 2) Разработка стандартов для валидации данных 3) Использование системы управления версиями (например, Git) с ограничениями по правам доступа 4) Определение ключевых метрики для мониторинга производительности модели и установите пороговые значения для их отслеживания | Git |