

Для функционирования ИС используются информационные ресурсы. Данные ресурсы могут быть подвержены вредоносному вмешательству извне. Для организации защиты используемой информации требуется произвести ее классификацию и привести краткое описание.

Для работы системы, технолог вводит данные о показателях работы оборудования. Из этого, в таблице 1 мы выделили два информационных объекта: конфиденциальные данные о работе оборудования и информация о сетевой инфраструктуре (интерфейсы, топология сети и т.д.). Система используется в ходе процесса мониторинга технологического оборудования рабочим персоналом. Следовательно, требуется хранить данные о пользователях ИС. Аудит информационных объектов приведен в таблице 1.

Таблица 1 – Аудит информационных объектов защиты

Объект	Профиль	№ п/п	Вид данных	Место
О ₁	Конфиденциальные данные о работе технологического оборудования	1	Справочная информация об оборудовании	Сервер БД
		2	Входная информация (Показатели работы оборудования/процесса)	
		3	Результаты работы аналитического блока системы	
О ₂	Информация о сетевой инфраструктуре	1	Данные о подключенных устройствах	ЛВС
О ₃	Личные данные обслуживающего персонала	1	Имена, должности сотрудников	Сервер БД

На основе аудита информационных объектов требуется провести их категорирование, то есть, оценить уровень возможного ущерба. Уровень ущерба рассчитывается по формуле 1.

$$S_i = K_i + C_i + A_i, \quad (1)$$

где: K_i – конфиденциальность;

A_i – целостность;

C_i – доступность.

Показатели K_i , A_i , C_i измеряются при помощи ранговой шкалы:

Конфиденциальность:

2 – «Высокая» – к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства Российской Федерации или информация, ограничение на распространение которой вводится решением руководства предприятия в соответствии с принятой политикой информационной безопасности.

1 – «Средняя» – к данной категории относится информация, не отнесенная к категории «Высокая», но ознакомление с которой посторонних лиц может нанести определенный ущерб (информация для служебного использования).

0 – «Нет требований» – к данной категории относится информация, обеспечение конфиденциальности которой не требуется.

Целостность:

2 – «Высокая» – к данной категории относится информация, несанкционированная модификация, удаление или фальсификация которой может привести к нанесению значительного прямого ущерба, целостность и аутентичность которой должна обеспечиваться

гарантированными методами в соответствии с обязательными требованиями действующего законодательства.

1 – «Средняя» – к данной категории относится информация, несанкционированная модификация, удаление или фальсификация которой может привести к нанесению незначительного косвенного ущерба, целостность которой должна обеспечиваться в соответствии с решением руководства.

0 – «Нет требований» – к данной категории относится информация, к обеспечению целостности которой требований не предъявляется.

Доступность:

2 – «Высокая» – доступ к информации должен осуществляться без существенных временных задержек в режиме online.

1 – «Средняя» – доступ к информации может обеспечиваться с существенными временными задержками, не препятствующими её использованию.

0 – «Низкая» – временные задержки при доступе к информации практически не лимитированы.

Таблица 2 – Категорирование информации

Объект	Профиль	Конфиденциальность	Целостность	Доступность (скорость доступа)	Итоговая категория
O ₁	Конфиденциальные данные о работе технологического оборудования	2	2	1	5
O ₂	Информация о сетевой инфраструктуре	2	2	1	5
O ₃	Личные данные обслуживающего персонала	2	1	0	3

Для выделенных информационных объектов требуется рассчитать вероятность их уязвимости. Для этого, выделим виды угроз, которые могут воздействовать на О. Возможны следующие виды угроз:

- утечка информации;
- модификация информации;
- уничтожение информации.

Для расчета вероятности уязвимости для каждого вида угроз, для каждого объекта требуется оценить возможность отражения атаки при помощи следующих методов:

- организационные;
- инженерно-технические;
- программно-аппаратные.

Для оценки используется ранговая система:

- 0 – невозможно ($P_{at} = 0$);
- 1 – только совокупность методов ($P_{at} = 0,25$);
- 2 – ограниченные совокупности ($P_{at} = 0,5$);
- 3 – практически возможно ($P_{at} = 0,75$);

– 4 – Полное парирование ($P_{at} = 1$).

Чтобы рассчитать вероятность уязвимости объекта для определенного типа угрозы требуется из одного вычесть максимальное значение P_{at} . Расчеты приведены в таблице 3.

Таблица 3 – Расчет вероятности уязвимости объекта

Угроза	Возможность отражения атаки P_{at}			Вероятность уязвимости объекта P_{ij} ($1 - \text{Max } P_{at}$)
	Организац. методы	Инженерно-технические	Программно-аппаратные	
Y_1 – утечка информации при воздействии на O_1	3	1	2	0,25
Y_1 – утечка информации при воздействии на O_2	2	0	2	$1 - 0,5 = 0,5$
Y_1 – утечка информации при воздействии на O_3	2	3	3	$1 - 0,75 = 0,25$
Y_1 – модификация информации при воздействии на O_1	3	2	3	$1 - 0,75 = 0,25$
Y_1 – модификация информации при воздействии на O_3	3	2	3	$1 - 0,75 = 0,25$
Y_1 – уничтожение информации при воздействии на O_1	2	1	1	$1 - 0,5 = 0,5$
Y_1 – уничтожение информации при воздействии на O_3	2	1	1	$1 - 0,5 = 0,5$

Для оценки рисков нанесения ущерба информационным объектам воспользуемся формулой:

$$R_i = P_i * \sum_j (P_{ij} * S_j), \quad (2)$$

где, P_i – вероятность реализации угрозы;

S_i – уровень ущерба.

Результаты расчетов приведены в таблице 4.

Таблица 4 – Анализ рисков и угроз

Угроза Y_i	Вероятность реализации угрозы P_i	Объект воздействия O_j	Вероятность уязвимости объекта P_{ij}	Уровень ущерба S_i	Оценка риска R_i
Y_1 – утечка информации	0,21	O_1	0,25	5	0,945
		O_2	0,5	5	
		O_3	0,25	3	
	0,26	O_1	0,25	5	0,52

Y ₂ – модификация информации		O ₃	0,25	3	
Y ₃ – уничтожение информации	0,34	O ₁	0,5	5	1,36
		O ₃	0,5	3	

По формуле 2 в таблице 4 была рассчитана оценка риска:

$$R_1 = 0,21 * (0,25*5 + 0,5*5 + 0,25*3) = 0,945;$$

$$R_2 = 0,26 * (0,25*5 + 0,25*3) = 0,52;$$

$$R_3 = 0,34 * (0,5*5 + 0,5*3) = 1,36.$$

Для реализации защиты от рисков и угроз, представленных в таблице 4 воспользуемся следующими типами мер защиты информации:

– организационные (административные) – ориентированы на регламентацию работы персонала. Важнейшей из них является политика безопасности, разрабатываемая индивидуально для каждого предприятия;

– правовые – предусматривают соблюдение законов и норм в области информационной безопасности с соблюдением законов и норм;

– аппаратно-программные – направлены на устранение угроз, непосредственно связанных с процессами хранения, обработки и передачи информации с помощью средств компьютерной техники;

– инженерно-технические – связаны с построением оптимальных сетей инженерных коммуникаций с учетом требований безопасности информации, а также основаны на применении специальных противопожарных средств, охранной сигнализации, визуального контроля обстановки в помещениях и на территориях.

В таблице 5 приведены конкретные меры из вышеуказанных типов.

Таблица 5 – Средства и методы защиты

Группа средств защиты	Название средства
Организационные	Организация надежной охраны помещения
	Организация проведения инструктажей сотрудников по правилам информационной безопасности
Правовые	Подписание каждым из сотрудников соглашения о неразглашении персональных данных согласно закону «О персональных данных» от 27.07.2007 №152-ФЗ
	Извещение каждого сотрудника при приеме на работу о распространении действия закона «Статьи 271-274 УК РФ от 13.06.1996 №63-ФЗ. Глава 28 Преступление в сфере компьютерной информации» в рамках данного предприятия
	Подписание каждым сотрудником документа, удостоверяющего его осведомленность о действии данного закона на территории организации и устанавливающего ответственность за совершение преступлений в сфере компьютерной информации
Аппаратно-программные	Установка антивируса на каждую рабочую станцию и сервера
	Установка источника бесперебойного питания к каждому серверу
	Осуществление резервного копирования данных каждый месяц
	Разграничение пользовательских прав доступа к данным
Инженерно-технические	Хранение коммутационных устройств в специальных шкафах
	Хранение серверов в серверной, с ограниченным доступом

Далее, разграничим доступ к информации из объектов защиты. Разграничение прав доступа представлено в таблице 6.

Таблица 6 – Разграничение доступа к информации

Объект	Сотрудник		
	Технолог	Оператор	Системный администратор
О ₁ - Данные о работе обор.			
Справочная информация об оборудовании	+	+	+
Показатели работы оборудования	+	+	+
Результаты работы аналитического блока	-	+	+
О ₂ - Инф о сетевой инфраструктуре			
Данные подключения к смежным системам	-	-	+
Данные об организации системы	-	-	+
О ₃ - Персональные данные			
Данные о сотрудниках	-	+	-

Выберем реализации средств защиты, описанных в таблице 5.

Для реализации средств защиты составим критерии, на основании которых будет осуществлен выбор.

Таблица 7 – Требования к реализации средств защиты

Наименование	Требование
ИБП	<ul style="list-style-type: none"> – эффективная выходная мощность: от 900 Вт – наличие обратной связи
Антивирус	<ul style="list-style-type: none"> – лицензированное ПО – возможность централизованного управления – автоматическая проверка подключения к сети и установка защищенного соединения
Утилита резервного копирования данных	<ul style="list-style-type: none"> – лицензированное ПО – возможность проверки целостности данных – централизованное управления – поддержка инкрементного резервного копирования

На основании таблицы 7 осуществим выбор реализаций средств защиты.

Таблица 8 – Реализации средств защиты

Средства защиты	Группа критериев				Цена
	1	2	3	4	
ИБП IPPON Smart Power PRO II Euo 2200	+	+	Нет требования	Нет требования	21 699 р.

Антивирусное средство Kaspersky для бизнеса Стандартный	+	+	+	Нет требования	28 625 р. на 10 узлов за 1 год
RuBackup	+	+	+	+	86 250 р.

Рассмотрим модели потенциальных нарушителей в таблице 9.

Таблица 9 – Модели нарушителей информационной безопасности

Тип	Внутренний нарушитель	Внешний нарушитель
Категория лиц	Сотрудник станции	Внешний хакер
Мотив	Нет мотива причинения вреда	Получение информации о ходе работе станции с целью дальнейшего саботажа на производстве
Намерения	Непреднамеренное нарушение безопасности информации из-за недостаточного понимания правил и политик безопасности.	Получение конфиденциальной информации о процессах производства
Квалификация	Сотрудник, который не имеет специализированного образования или опыта в области информационной безопасности	Способность обходить существующие защитные механизмы и обнаруживать уязвимости
Знание о системе	Является пользователем системы	Нет данных о системе
Характер действий	Непреднамеренное удаление или изменение важных данных из-за ошибок при работе с системами	Сканирование сети предприятия для выявления уязвимостей и слабых мест
Наиболее вероятные угрозы	Незаконное удаление или изменение данных	Утрата конфиденциальности данных
Время действия	Время функционирования системы	Время функционирования системы
Место действия	Цех, где работает сотрудник	За пределами предприятия