Таблица 1.

Объект защиты для ВАШЕГО ОБЪЕКТА	Нарушение Целостности	Нарушение доступности	Нарушение конфиденциальности
Бумажная документация	Замена модифицированной копией, частичная порча	Кража, уничтожение	Несанкционированное копирование: фотографирование, ксерокопирование, сканирование и т.д.
Электронная документация	Замена модифицированной копией	Порча формата хранения, удаление из хранилища	Несанкционированное копирование.
Линия сборки	Изменение параметров работы линии на неоптимальные Физическая поломка Кража частей/деталей	Отключение устройств линии, повреждение сети	Фотографирование, копирование схемы работы, копирование микропрограмм
Система АСУ ТП	Модификация кода ПО АСУ ТП. Модификация данных. Взлом системы защиты (например, от перемещения станков)	Отключение серверов, повреждение сети, DOS и DDOS атаки	Несанкционированный доступ к системе, копирование кода, копирование данных
Система мониторинга	Подделка / модификация данных от датчиков. Модификация кода ПО.	Отключение серверов, повреждение сети, DOS и DDOS атаки	Несанкционированный доступ к системе, копирование кода.
База данных	Изменение и/или частичное удаление данных. Изменение структуры: таблиц, хранимых процедур, триггеров и других объектов	Отключение серверов, повреждение сети, DOS и DDOS атаки, удаление пользователей и/или прав.	Несанкционированный доступ к системе, копирование базы (данных и структуры данных)
Файловое хранилище	Изменение или частичное удаление файлов (данных в них)	Отключение серверов, повреждение сети, DOS и DDOS атаки, удаление пользователей и/или прав.	Несанкционированный доступ к системе, копирование файлов (данных)
Система безопасности	Модификация кода ПО, взлом системы защиты, модификация/подделка	Отключение серверов, повреждение сети, DOS и DDOS атаки,	Несанкционированный доступ к системе, копирование кода ПО, копирование данных

	данных (инцидентов безопасности)	повреждение/отключение устройств (например, камер)	(инцидентов безопасности)

Таблица 2.

Инф. ресурсы	Наиболее серьезные последствия	Сценарий
Линия сборки	Физическая поломка. Ущерб экологии, жизни и здоровья людей	1. Сбор информации из открытых источников о потенциальных объектах для атаки: работниках, которые потенциально имеют доступ к линии сборки 2. С помощью методов целевого фишинга (с помощью письма с внедренным во вложение кодом загрузчика) получение доступа к системе одного из работников изнутри. 3. Проверка, что загрузчик получил доступ к компьютеру нужного сотрудника – у которого есть доступ к линии сборки 4. Загрузка загрузчиком тела дроппера из сети. 5. Подключение дроппером к линии сборки и замена модификация ее программного кода. 6. Стирание дроппером себя из внедренной системы. 7. Активация измененного программного кода линии сборки при наступлении некоторого события (например, времени). Выход линии сборки из строя.
Электронная документация	Кража секретных и конфиденциальных данных. Экономический и репутационный ущерб	1. Сбор информации из открытых источников о потенциальных объектах для атаки: инженеров предприятия, которые могут иметь доступ к секретным/конфиденциальным данным. 2. С помощью методов социальной инженерии, хакер через мессенджер (telegram) списывается с одним из инженеров, представляется, что он один из системных администраторов предприятия и пересылает ему документ, с которым тот должен ознакомиться. 3. Документ содержит зловредный код для создания backdoor, через который хакер мог бы подключиться к компьютеру.

		4. Инженер открывает этот документ и читает его. Зловредный код устанавливает backdoor. 5. Хакер через этот backdoor подключается к компьютеру работника, сканирует его и скачивает всю интересующую его информацию. 6. Хакер продает скаченную информацию фирме конкуренту или спецслужбам других стран.
Система мониторинга	Подмена данных от датчиков линии сборки, что может привести к невозможности правильной оценки ситуации со стороны персонала и ее поломке. А также к аварии с ущербом экологии, жизни и здоровья людей	1. Внутренний нарушитель звонит по телефону одному из работников, который имеет доступ к системе мониторинга и представляется ему системным администратором. 2. Внутренний нарушитель просит работника сказать свои логин и пароль от компьютера якобы для решения некоторых задач администрирования (вишинг). 3. Работник дает ему эти данные. 4. Внутренний нарушитель подключается с помощью этих данных к компьютеру работника. 5. Внутренний нарушитель находит конфигурационный файл системы мониторинга и перенастраивает его так, чтобы данные с датчиков либо не снимались вообще, либо снимались крайне редко. 6. В какой-то момент времени на линии сборки происходит неполадка. Но система мониторинга ничего не показывает. Как итог, линия сборки ломается.
Система безопасности	Возможность физического проникновения на предприятие, которое будет не замечено со стороны охраны	1. Злоумышленники разбрасывают рядом с предприятием переносные накопители (флэш карты) с установленным на них зловредным ПО (атака “дорожное яблоко”). 2. Некоторые работники подбирают эти переносные накопители и проверяют их на своих рабочих компьютерах. 3. При подключении такого переносного накопителя к компьютеру на него устанавливается специальный backdoor код. 4. Хакер подключается через этот backdoor код к компьютеру.

		5. Хакер сканирует внутреннюю сеть предприятия, находит сервер, отвечающий за видеонаблюдение, и отключает камеры. 6. Группа преступников ночью проникает на территорию предприятия по пути, на котором нет камер и осуществляет кражу готовых изделий.
База данных отдела кадров	Кража персональных данных работников предприятия с последующей продажей их преступным группировкам	1. Внутренний нарушитель при посещении отдела кадров подсмотрел логин и пароль подключения к БД с персональными данными. 2. Подключение к этой БД с помощью подсмотренных логина и пароля. 3. Создание резервной копии (backup) БД с персональными данными. 4. Копирование созданной резервной копии БД с сервера на компьютер нарушителя по сети. 5. Копирование созданной резервной копии БД с компьютера нарушителя на переносной накопитель. 6. Вынос переносного накопителя с территории предприятия. 7. Продажа скопированных персональных данных работников предприятия через даркнет.

Таблица 3.

№	Этапы	Что делаем
1	Согласование с руководством	Объяснение руководству, что такое фишинг. Какие есть риски, если ничего не делать: потеря персональных данных, потеря секретных и конфиденциальных данных, доступ во внутреннюю сеть предприятия. И как результат: финансовые и репутационные потери, утечка секретных и конфиденциальных данных, нарушение безопасности, аварии на производстве. Составляем и согласовываем с руководством план дальнейших действий, который включает в себя обучение персонала и периодические проверки. Важно, чтобы информация о тестировании оставалась секретной для персонала, в противном случае мы получим совсем не те результаты.
2	Составление писем	Создаем 2 группы писем для проверки на общий и на целевой фишинг. Письма для проверки на общий фишинг являются обезличенными и могут содержать предложение скидок,

		общее анкетирование, рассылку фотографий, требования от группы системных администраторов на запуск некоторого скрипта и т.д. Письма для проверки на целевой фишинг должны быть адресованы конкретному лицу и могут содержать просьбы, предложения или требования именно к этому лицу – например, просьба логина/пароля от системы, эксклюзивные скидки от знакомого, просьба переслать тот или иной файл, требования от группы системных администраторов на запуск некоторого скрипта и т.д. В любом случае, все ссылки должны ввести на подставные страницы, файлы содержать некоторый код, фиксирующий на сервере его запуск и т.д.
3	Рассылка писем	Периодически (согласно плану, согласованному с руководством) происходит рассылка писем обеих групп. Письма для проверки на общий фишинг рассылаются всем. Письма для проверки на целевой фишинг рассылаются некоторой выбранной группе лиц – преимущественно тем, кто обладает особыми привилегиями и у кого есть доступ к чувствительной информации.
4	Сбор данных. Мониторинг	Сбор данных осуществляется следующими способами: 1. Если на фишинговое письмо ожидается ответ (например, с некоторым файлом), то мы должны автоматически отслеживать почтовые ящики, с который производилась рассылка, а также содержимое ответных писем: прислал ли сотрудник в ответ на наше фишинговое письмо некоторый файл с данными или нет и т.д. 2. Если фишинговое письмо содержало ссылку, то мы отслеживаем какие пользователи перешли по этой ссылке и какие данные они оставили. 3. Если фишинговое письмо содержало вложение (с кодом, который фиксировал на сервере его запуск), то мы смотрим кто и сколько раз этот код запускал.
5	Подведение итогов	Обрабатываем полученные данные: смотрим, кто из сотрудников попался на фишинговое письмо, обращая особое внимание на тех, кто ввел или переслал чувствительную информацию. На основе полученной информации можно сделать выводы насколько хорошо работает защита ИБ в компании и, возможно, пересмотреть ее некоторые подходы и политики
6	Обучение	Обучение должно проводиться для всего персонала: как теоретическое, так и практическое с объяснениями конкретных случаев. Для персонала, который попался на фишинговые письма при проверке стоит проводить отдельное дополнительное обучение. Также отдельное дополнительное обучение стоит провести с тем персоналом, кто обладает особыми привилегиями и у кого есть доступ к чувствительной информации
7	Повторное тестирование	Через некоторое время после обучения проводим повторное тестирование (не связанное с периодической

		рассылкой). Письма рассылаем всем сотрудникам, кто попался на фишинг в прошлый раз.

Таблица 4.

Название должности	Пример целевого фишингового письма	Эмоции от письма
Бухгалтер	Уважаемая Мария Ивановна, срочно обновите вашу систему – в противном случае, завтра вы не сможете зайти в 1С. Для обновления нажмите на ссылку. С уважением, системный администратор Иванов И.И.	Важность, срочность, испуг
Сотрудник отдела кадров	Уважаемая Мария Ивановна, сегодня и только сегодня скидка на всю продукцию Дольче Габбана у нас 90%. Для получения этой скидки пройдите по ссылке в письме и зарегистрируйтесь. С уважением, торговый дом “ДольчеГаббана”	Срочность, жадность
Системный администратор	Уважаемый Иван Иванович, мы заметили по логам, что ваш антивирус обновляется не совсем корректно. Для исправления ситуации, запустите приложенный в письме скрипт. С уважением, служба мониторинга Лаборатории Касперского.	Важность, ответственность
Инженер	Уважаемый Иван Иванович, при сборке изделия с артикулом АД-666 у нас возникли серьезные проблемы. Возможно, у нас неправильный чертеж. Не могли бы выслать актуальную версию сборочного чертежа как можно скорее, т.к. у нас срок окончания сборки сегодня. С уважением, сборщик изделий Семенов С.С.	Важность, срочность, ответственность
Оператор линии сборки	Уважаемый Иван Иванович, ваша учетная запись требует подтверждения – в противном случае завтра она будет заблокирована. Для ее подтверждения пройдите по ссылке в письме. С уважением, системный администратор Семенов С.С.	Важность, срочность, испуг
Сотрудник экономического отдела	Уважаемая Мария Ивановна, ваша учетная запись на портале закупок была заблокирована. Для ее разблокировки пройдите по ссылке и заполните анкету с личными данными. С уважением, системный администратор Семенов С.С.	Важность, срочность, испуг

Таблица 5.

ИР для защиты	Сценарии нарушителей

Линия сборки	1. Злоумышленник собирает информацию из открытых источников о потенциальных объектах для атаки: работниках, которые потенциально имеют доступ к линии сборки. 2. Злоумышленник рассылает письмо работникам, о которых он нашел информацию, с просьбой, например, пройти по ссылке (целевой фишинг). 3. Один из работников проходит по ссылке – на его компьютер загружается вредоносное ПО. 4. Вредоносное ПО проверяет, что с компьютера этого работника есть доступ к линии сборки 5. Вредоносное ПО модифицирует программный код линии сборки, чтобы она сломалась, например, в 11 утра следующего дня. 6. Вредоносное ПО стирает себя из системы.
База данных отдела кадров	1. Злоумышленник сканирует веб сервер предприятия и находим в нем 0-day уязвимость. 2. Злоумышленник через 0-day уязвимость получает доступ к веб серверу. 3. Злоумышленник ищет, что еще находится на веб сервере и находит на нем сервер баз данных. 4. Злоумышленник атакой по словарю подбирает пароль для стандартного логина. 5. Злоумышленник проверяет сервер баз данных и находит базу отдела кадров. 6. Злоумышленник создает резервную копию этой базы и скачивает его себе
Система мониторинга	1. Работник скачивает на свой рабочий компьютер с торрентов компьютерную игру 2. Игра оказывается заражена вирусом шифровальщиком. При запуске установщика этой игры вирус заражает компьютер работника. 3. Вирус шифровальщик зашифровывает файловую систему на компьютере работника. 4. Работник в этот момент был подключен к серверу мониторинга с повышенными правами. 5. Вирус шифровальщик попадает на сервер мониторинга и заражает его. 6. Вирус шифровальщик зашифровывает файловую систему на сервере мониторинга
Система видеонаблюдения	1. Злоумышленник раскидывает радом с территорией предприятия переносные накопители (флэш карты) с установленным на них вредоносным ПО (атака “дорожное яблоко”). 2. Некоторые сотрудники подбирают эти переносные носители и вставляют их в свои рабочие компьютеры 3. Вредоносное ПО активируется, создает backdoor и передает сигнал злоумышленнику. 4. Злоумышленник подключается через этот backdoor к рабочему компьютеру. 5. Злоумышленник поиском по локальной сети находит сервер видеонаблюдения

	6. Злоумышленник подбирает пароль к этому серверу, входит на него и стирает архив записей системы видеонаблюдения за последний месяц. 7. Злоумышленник отключается от сервера, уничтожает backdoor и выходит из системы

Таблица 6.

Найденные недостатки	Как исправить
Рабочее место оператора пульта охраны	
1. Наличие возможности на рабочем месте запускать сторонние приложения, например, игры.	Использование списка разрешенных для запуска приложений: что не разрешено, то запрещено. Логирование всех действий пользователя
2. Наличие возможности выходить в сеть Интернет на рабочем месте.	Либо запрет выхода в интернет на уровне сетевого оборудования, либо подключение к сегменту сети, который не соединен с сетью Интернет.
3. Наличие возможности приносить и вставлять свои внешние накопители.	Физическое блокирование портов на системном блоке рабочего места. Логирование всех действий пользователя
4. Слишком много мониторов на одного охранника: как итог – важные события могут быть им пропущены	Наем большего количества охранников – как итог, количество мониторов (и мест), за которыми должен следить один охранник должно быть уменьшено
Комната администраторов	
1. Отсутствие политики блокирования компьютера при отсутствии администратора за своим рабочим местом: в этом случае, любой, кто попадет за рабочее место администратора сможет сделать все то же, что и администратор – например, получить доступ к конфиденциальным данным, устроить диверсию и т.п.	Введение политики обязательного блокирования рабочего места при отсутствии работника за ним – со штрафными санкциями, если будет обнаружено ее несоблюдение. Введение политики обязательного автоматического блокирования рабочего места в случае короткого периода бездействия пользователя
2. Использование стороннего ПО. Стороннее ПО, особенно полученное из не надежных источников, часто является переносчиком разнообразного вредоносного ПО. Особенно опасно, когда	Запрет установки стороннего ПО без согласования со службой ИБ. Запрет установки ПО не из официальных репозиториев или без подписи.

такое ПО используют люди, входящие в систему с повышенными привилегиями.	
3. Запрет на использование оборудования компании для личных целей, например, для игр (project beyond)	Запрет установки стороннего ПО без согласования со службой ИБ. Использование списка запрещённых приложений. Логирование всех действий.
4. Хранение конфиденциальной информации в открытом виде: в виде бумажек, наклеенных на монитор	Запрет хранения конфиденциальной информации в таком виде: использование, например, менеджера паролей для хранения данных аутентификации
АРМ системного администратора	
1. Хранение конфиденциальной информации в открытом виде: в виде бумажек, наклеенных на монитор	Запрет хранения конфиденциальной информации в таком виде: использование, например, менеджера паролей для хранения данных аутентификации
2. Возможная потеря важных данных: если бумажка отклеится и упадет, то с большей долей вероятности важная информация будет потеряна и для ее восстановления придется затратить значительные усилия	Запрет хранения любой (в том числе и конфиденциальной информации) в таком виде: использование для хранения более надежных электронных средств – менеджеры паролей, документы, клиент-серверные системы для хранения текстовых и других данных
3. В случае каких-либо проблем (например, в связи с болезнью) с администратором, работающим за данным местом, его не легко заменить другим администратором, так вся информация находится в виде бумажек на мониторе	Запрет хранения любой (в том числе и конфиденциальной информации) в таком виде: для задач использовать баг-трекер, для знаний – например wiki, для хранения конфиденциальной информации – менеджеры паролей.
4. Отсутствие политики блокирования компьютера при отсутствии администратора за своим рабочим местом: в этом случае, любой, кто попадет за рабочее место администратора сможет сделать все то же, что и администратор – например, получить доступ к конфиденциальным данным, устроить диверсию и т.п.	Введение политики обязательного блокирования рабочего места при отсутствии работника за ним – со штрафными санкциями, если будет обнаружено ее несоблюдение. Введение политики обязательного автоматического блокирования рабочего места в случае короткого периода бездействия пользователя
5. Использование монитора, с которого легко снять электромагнитное излучение и	Использовать мониторы с меньшим уровнем излучения – например, жидкокристаллические. Использовать в комнате, в которой располагается рабочее

получить доступ к тому, что он показывает.	место администратора специальную защиту от снятия электромагнитного излучения (клетку Фарадея).
6. На рабочем месте администратора стоит не самое свежее ПО или не стоят актуальные обновления для ПО. Это означает, что ПО на рабочем месте администратора имеет известные уязвимости, для эксплуатации которых можно найти решения в сети даркнет.	Всегда по возможности либо ставить самое свежее ПО, либо ставить самые актуальные обновления. Это защитит, по крайней мере от известных уязвимостей.

Таблица 7.

Найденные недостатки	Как исправить
Отсутствуют ограничения на сложность пароля. Это означает, что пароль пользователя может быть легко подобран атакой подбором по словарю	Введение требований по сложности к паролю: минимальная длина, обязательно использовать символы как минимум из 3 групп (например, буквы, цифры, знаки) и т.д. Валидация пароля согласно введенным требованиям при его создании/изменении
Отсутствие обязательного периодического изменения пароля пользователя. Если пароль пользователя будет однажды скомпрометирован, то он останется скомпрометированным, пока пользователь его не поменяет, то есть на неопределенное время	Введение срока действия пароля: если у учетной записи срок действия пароля истек, то в данную учетную запись с истекшим паролем зайти будет нельзя – нужно будет обязательно поменять пароль. Введение истории паролей пользователей: чтобы пользователь не ограничивался использованием только двух паролей
Отсутствие многофакторной аутентификации. Если пароль будет скомпрометирован, то злоумышленники без проблем смогут им воспользоваться и войти в систему	Введение многофакторной аутентификации сильно усложняет злоумышленнику вход в систему в случае компрометации пароля. Обучение пользователя распознаванию методов социальной инженерии (используемых злоумышленником для того, чтобы узнать данные других факторов в многофакторной аутентификации) делают компрометацию пароля практически бесполезной для злоумышленника.

Использование одного пароля во всех системах. Если злоумышленники смогут скомпрометировать пароль пользователя, то по нему они смогут войти во все системы сразу	Введение политики использования разных паролей для каждой системы усложнит злоумышленникам жизнь. Как вариант – можно внедрить систему управления паролями, которая генерирует одноразовые пароли для входа пользователя в систему. Либо, использовать единую точку входа (с одним паролем), но с обязательным наличием многофакторной аутентификации
Пин код меняется достаточно редко. Если пин код будет скомпрометирован злоумышленником в начале месяца, то практически весь месяц злоумышленник будет иметь доступ в закрытую зону	Уменьшить срок смены пин кода хотя бы на раз в неделю. Обязательно поставить видеонаблюдение в закрытую зону, чтобы узнать о проникновении в нее злоумышленников
Получение одноразового пароля к онлайн банкингу слишком простое. Такую информацию о пользователе, как фамилию, номер паспорта и дату рождения легко можно найти из слитых баз (например, у операторов сотовой связи) в даркнете, либо получить с помощью методов социальной инженерии. Более того – эту информацию можно подслушать.	Изменить схему подключения к онлайн банкингу – например, использовать обычную многофакторную аутентификацию без запроса персональных данных пользователя по телефону.

Таблица 8.

Элемент атаки, тактика по МИТРЕ	Способ реализации нарушителем, № техники по МИТРЕ	Мера защиты
Сценарий: Разработка удаленного управления TA0001 Initial Access	T1659 Content Injection: внедрение вредоносного контента в систему через сетевой трафик.	M1041 Encrypt Sensitive Information: защита чувствительной информации с помощью шифрования M1021 Restrict Web-Based Content: ограничение на использование определенных веб-сайтов, блокировка загрузок/вложений, блокировка Javascript, ограничение расширений браузера и т. д.

Сценарий: Разработка удаленного управления TA0001 Initial Access	T1189 Drive-by Compromise: получение доступ к системе через пользователя, посещающего веб-сайт в ходе обычного просмотра	M1048 Application Isolation and Sandboxing: Ограничение выполнение кода виртуальной средой в конечной системе или при передаче в нее. M1050 Exploit Protection: использование возможности для обнаружения и блокирования условий, которые могут привести к возникновению уязвимости программного обеспечения или быть ее признаком. M1021 Restrict Web-Based Content: ограничение на использование определенных веб-сайтов, блокировка загрузок/вложений, блокировка Javascript, ограничение расширений браузера и т. д. M1051 Update Software: регулярное обновление программное обеспечение, чтобы снизить риск эксплуатации уязвимостей.
Сценарий: Повышение привилегий TA0004 Privilege Escalation	T1548 Abuse Elevation Control Mechanism: обход механизмов, предназначенных для контроля повышения привилегий, чтобы получить разрешения более высокого уровня.	M1047 Audit: проведение аудита или сканирования систем, разрешений, небезопасного программного обеспечения, небезопасных конфигураций и т. д. для выявления потенциальных уязвимостей. M1038 Execution Prevention : блокирование выполнения кода в системе с помощью контроля приложений и/или блокировки скриптов. M1028 Operating System Configuration: внесение изменений в конфигурацию, связанные с операционной системой или общей функцией

		операционной системы, которые приведут к повышению устойчивости системы к различным методам взлома. M1026 Privileged Account Management: управление созданием, изменением, использованием и разрешениями, связанными с привилегированными учетными записями, включая SYSTEM и root. M1022 Restrict File and Directory Permissions: ограничение доступа, установлением разрешений для каталогов и файлов, которые не являются специфическими для пользователей или привилегированных учетных записей. M1051 Update Software: регулярное обновление программное обеспечение, чтобы снизить риск эксплуатации уязвимостей.
Сценарий: Разведка TA0043 Reconnaissance	T1595 Active Scanning: выполнение активного разведывательного сканирование для сбора информации, которая может быть использована во время нацеливания	Минимизация информации, которую можно получить во время активного сканирования (M1056 Pre-compromise: эту технику нельзя легко смягчить с помощью превентивного контроля, поскольку она основана на поведении, осуществляемом за пределами сферы действия корпоративных защит и контроля; усилия должны быть сосредоточены на минимизации объема и чувствительности данных, доступных внешним сторонам.)

Таблица 9.

№ политики	Название	Текущее состояние ВАШЕГО ОБЪЕКТА	Что нужно сделать для формирования политики ВАШЕГО ОБЪЕКТА
A.5	Политики информационной безопасности		
A.5.1.1	Политики ИБ	Соблюдается Устарело	1. Сформировать полный комплекс актуальных на данный момент времени политик ИБ. 2. Сформировать документацию, полностью описывающую сформированный комплекс политик ИБ 3. Донести сформированный комплекс политик ИБ до персонала. Получить подпись об ознакомлении от каждого сотрудника. 4. Провести обучение персонала новому комплексу политик ИБ.
A.5.1.2	Пересмотр политик информационной безопасности	Не соблюдается	1. Установить порядок и периодичность планового пересмотра комплекса политик ИБ. Назначить ответственного. 2. Установить порядок и периодичность внеочередного (например, из-за изменения законодательства РФ) пересмотра комплекса политик ИБ. Назначить ответственного.

A6	Организация информационной безопасности		
A.6.1	Внутренняя организация		
A.6.1.1	Должностные функции и обязанности, связанные с информационной безопасностью	Соблюдается	
A.6.1.2	Разделение обязанностей	Соблюдается частично	1. Провести текущий анализ распределения ролей среди персонала. 2. На основе этого анализ определить, на каких позициях и для каких ролей наблюдаются проблемы с разделением обязанностей. 3. Определить, можно ли назначить часть обязанностей другим работникам без создание новых проблем и конфликтов с их существующими обязанностями (например, проверяющий не должен проверять сам себя). 4. Определить нужны ли предприятию еще сотрудники. Если да, то сформировать список требований к новым сотрудникам.
A.6.1.3	Контакты с полномочными органами	Соблюдается	
A.6.1.4	Контакты с профессиональными сообществами	Соблюдается	

A.6.1.5	Информационная безопасность в управлении проектами	Соблюдается	
A.6.2	Мобильные устройства и удаленная работа		
A.6.2.1	Политика в отношении мобильных устройств	Соблюдается	
A.6.2.2	Удаленная работа	Соблюдается	
A.7	Безопасность персонала		
A.7.1.1	Предварительная проверка	Соблюдается	
A.7.1.2	Условия трудового соглашения	Соблюдается	
A.7.2	В период занятости	Соблюдается	
A.7.2.1	Ответственность руководства	Соблюдается	
A.7.2.2	Осведомленность, образование и обучение в сфере информационной безопасности	Соблюдается	
A.7.2.3	Дисциплинарные меры	Соблюдается частично.	1. Провести ревизию дисциплинарных мер, применяемых сейчас. 2. На основе этой ревизии сформировать четкую документацию по применяемым дисциплинарным мерам: за какие действия какие меры должны быть применены к сотруднику. 3. Донести эту информацию до персонала. Получить подпись об ознакомлении от каждого сотрудника.

A.7.3	Прекращение и изменение трудовых отношений	Соблюдается	
A.7.3.1	Освобождение от обязанностей или их изменение	Соблюдается	
A.8	Управление активами		
A.8.1	Ответственность за активы	Соблюдается	
A.8.1.1	Инвентаризация активов	Соблюдается	
A.8.1.2	Владение активами	Соблюдается	
A.8.1.3	Надлежащее использование активов	Соблюдается	
A.8.1.4	Возврат активов	Соблюдается	
A.8.2	Классификация информации		
A.8.2.1	Классификация информации	Соблюдается	
A.8.2.2	Маркировка информации	Соблюдается	
A.8.2.3	Обращение с активами	Соблюдается	
A.8.3	Обращение с носителями информации		
A.8.3.1	Управление съемными носителями	Соблюдается	
A.8.3.2	Утилизация носителей информации	Не соблюдается	1. Написать регламент, определяющий, когда, как и кем должна проводиться утилизация носителей 2. Создать группу по утилизации носителей на территории предприятия. 3. Выделить этой группе помещение, закупить

			оборудование, нанять персонал. 4. Донести информацию об утилизации носителей до персонала. Получить подпись об ознакомлении от каждого сотрудника.
A.8.3.3	Физическое перемещение носителей информации	Соблюдается	
A.9	Контроль доступа		
A.9.1	Диктуемые бизнесом требования к контролю доступа		
A.9.1.1	Политика контроля доступа	Соблюдается	
A.9.1.2	Доступ к сетям и сетевым службам	Соблюдается	
A.9.2	Управление доступом пользователей		
A.9.2.1	Регистрация и отмена регистрации пользователя	Соблюдается	
A.9.2.2	Предоставление доступа пользователю	Соблюдается	
A.9.2.3	Управление привилегированными правами доступа	Соблюдается	
A.9.2.4	Управление секретной информацией аутентификации пользователей	Соблюдается	
A.9.2.5	Пересмотр прав доступа пользователей	Соблюдается	
A.9.2.6	Отмена или изменение прав доступа	Соблюдается	

A.9.3	Обязанности пользователей		
A.9.3.1	Использование секретной информации аутентификации	Соблюдается	
A. 9.4	Контроль доступа к системе и приложениям	Соблюдается	
A.9.4.1	Ограничение доступа к информации	Соблюдается	
A.9.4.2	Безопасные процедуры входа в систему	Соблюдается	
A.9.4.3	Система управления паролями	Соблюдается	
A.9.4.4	Использование утилит с привилегированными правами	Соблюдается	
A.9.4.5	Контроль доступа к исходным кодам	Соблюдается	
A.10	Криптография		
A.10.1	Криптографические методы защиты		
A.10.1.1	Политика использования криптографических методов защиты	Соблюдается	
A.10.1.2	Управление ключами	Соблюдается	
A.11	Физическая безопасность и защита от природных угроз		
A.11.1	Охраняемая зона		
A.11.1.1	Физический периметр безопасности	Соблюдается	

A.11.1.2	Средства контроля прохода	Соблюдается	
A.11.1.2	Средства контроля прохода	Соблюдается	
A.11.1.4	Защита от внешних угроз и угроз природного характера	Соблюдается	
A.11.1.5	Работа в охраняемых зонах	Соблюдается	
A.11.1.6	Зоны доставки и отгрузки	Соблюдается	
A.11.2	Оборудование		
A.11.2.1	Размещение и защита оборудования	Соблюдается	
A.11.2.2	Службы обеспечения	Соблюдается	
A.11.2.3	Защита кабельных сетей	Соблюдается	
A.11.2.4	Обслуживание оборудования	Соблюдается	
A.11.2.5	Вынос активов	Соблюдается частично	1. Провести ревизию существующих активов, которые могут быть вынесены. 2. Если будут обнаружена недостача (крупная), то провести расследование и наказать виновных. 3. Разработать регламент по работе с активами: когда и кому можно их выносить, какие документы для этого нужны и т.д. 4. Разработать регламент для охраны на досмотр вносимых и выносимых вещей: что можно вносить и выносить, что нельзя, в каких случаях нужна проверка.

			4. Донести эту информацию до персонала. Получить подпись об ознакомлении от каждого сотрудника. 5. Разработать регламент плановых и внезапных проверок активов. Назначить ответственного
A.11.2.6	Защита оборудования и активов вне территории	Соблюдается	
A.11.2.7	Безопасная утилизация или повторное использование оборудования	Соблюдается	
A.11.2.8	Оборудование пользователя, оставленное без присмотра	Соблюдается	
A.11.2.9	Политика чистого стола и чистого экрана	Соблюдается	
A.12	Безопасность производственной деятельности		
A.12.1	Рабочие процедуры и обязанности		
A.12.1.1	Документированные рабочие процедуры	Соблюдается	
A.12.1.2	Управление изменениями	Соблюдается	
A.12.1.2	Управление изменениями	Соблюдается	
A.12.1.4	Разделение среды разработки, тестирования и эксплуатации	Соблюдается	
A.12.2	Защита от вредоносного кода		
A.12.2.1	Меры защиты от вредоносного кода	Соблюдается	

A.12.3	Резервное копирование		
A.12.3.1	Резервное копирование информации	Соблюдается	
A.12.4	Ведение журналов и мониторинг		
A.12.4.1	Регистрация событий	Соблюдается	
A.12.4.2	Защита информации в журналах	Соблюдается	
A.12.4.3	Журналы действий администратора и оператора	Соблюдается	
A.12.4.4	Синхронизация часов	Соблюдается	
A.12.5	Контроль эксплуатируемого программного обеспечения		
A.12.5.1	Установка программ в эксплуатируемых системах	Соблюдается	
A.12.6	Управление техническими уязвимостями		
A.12.6.1	Управление техническими уязвимостями	Соблюдается	
A.12.6.2	Ограничения на установку программного обеспечения	Соблюдается	
A.12.7	Ограничения на аудит информационных систем		
A.12.7.1	Средства управления аудитом информационных систем	Соблюдается	
A.13	Безопасность обмена информацией		

A.13.1	Управление сетевой безопасностью		
A.13.1.1	Средства управления сетями	Соблюдается	
A.13.1.2	Безопасность сетевых сервисов	Соблюдается	
A.13.1.3	Разделение в сетях	Соблюдается	
A.13.2	Передача информации		
A.13.2.1	Политики и процедуры передачи информации	Соблюдается	
A.13.2.2	Соглашения по передаче информации	Соблюдается	
A.13.2.3	Электронные сообщения	Соблюдается	
A.14	Приобретение, разработка и обслуживание систем		
A.14.1	Требования по безопасности информационных систем		
A.14.1.1	Анализ и установление требований по информационной безопасности	Соблюдается	
A.14.1.2	Безопасность прикладных услуг в сетях общего пользования	Соблюдается	
A.14.1.3	Защита операций прикладных услуг	Соблюдается	
A.14.2	Безопасность в процессах разработки и поддержки		
A.14.2.1	Политика безопасности при разработке	Соблюдается	

A.14.2.2	Процедуры управления системными изменениями	Соблюдается	
A.14.2.3	Технический анализ приложений после изменений операционной платформы	Соблюдается	
A.14.2.4	Ограничения на изменения в пакетах программ	Соблюдается	
A.14.2.5	Принципы разработки защищенных систем	Соблюдается	
A.14.2.6	Безопасная среда разработки	Соблюдается	
A.14.2.7	Разработка, переданная на аутсорсинг	Соблюдается	
A.14.2.8	Тестирование защищенности системы	Соблюдается	
A.14.2.9	Приемочное тестирование системы	Соблюдается	
A.14.3	Данные для тестирования		
A.14.3.1	Защита данных для тестирования	Соблюдается	
A.15	Отношения с поставщиками		
A.15.1	Информационная безопасность в отношениях с поставщиками		
A.15.1.1	Политика информационной безопасности в отношениях с поставщиками	Соблюдается	
A.15.1.2	Решение вопросов безопасности в	Соблюдается	

	соглашениях с поставщиками		
A.15.1.3	Цепочка поставок информационно-коммуникационных технологий	Соблюдается	
A.15.2	Управление предоставлением услуги поставщиком	Соблюдается	
A.15.2.1	Мониторинг и анализ услуг поставщика	Соблюдается	
A.15.2.2	Управление изменениями в услугах поставщика	Соблюдается	
A.16	Управление инцидентами информационной безопасности		
A.16.1	Управление инцидентами информационной безопасности и улучшения		
A.16.1.1	Обязанности и процедуры	Соблюдается	
A.16.1.2	Оповещение о событиях, связанных с информационной безопасностью	Соблюдается	
A.16.1.3	Оповещение об уязвимостях в информационной безопасности	Соблюдается	
A.16.1.4	Оценка и решение по событиям информационной безопасности	Соблюдается	
A.16.1.5	Ответные меры на инциденты информационной безопасности	Соблюдается	

A.16.1.6	Излечение уроков из инцидентов информационной безопасности	Соблюдается	
A.16.1.7	Сбор свидетельств	Соблюдается	
A.17	Аспекты информационной безопасности в менеджменте непрерывности бизнеса		
A.17.1	Непрерывность информационной безопасности		
A.17.1.1	Планирование непрерывности информационной безопасности	Соблюдается	
A.17.1.2	Обеспечение непрерывности информационной безопасности	Соблюдается	
A.17.1.3	Проверка, анализ и оценка непрерывности информационной безопасности	Соблюдается	
A.17.2	Резервирование		
A.17.2.1	Возможность применения средств обработки информации	Соблюдается	
A.18	Соответствие		
A.18.1	Соответствие законодательным и контрактным требованиям	Соблюдается	
A.18.1.1	Определение действующих законодательных и контрактных требований	Соблюдается	

A.18.1.2	Права интеллектуальной собственности	Соблюдается	
A.18.1.3	Защита записей	Соблюдается	
A.18.1.4	Конфиденциальность и защита персональных данных	Соблюдается	
A.18.1.5	Регламентация применения криптографических методов	Соблюдается	
A.18.2	Анализ информационной безопасности		
A.18.2.1	Независимый анализ информационной безопасности	Соблюдается	
A.18.2.2	Соответствие политикам безопасности и стандартам	Соблюдается	
A.18.2.3	Анализ технического соответствия	Соблюдается	

Таблица 10.

Инф. ресурсы	Меры по защите
Бумажные чертежи и документация	Хранение документов в специальных сейфах; выдает их персонал со специальным допуском. Аутентификация и авторизация работников по пропуску. Использование специально отведенных комнат для работы с секретной и конфиденциальной документацией. Запрет проноса на территорию предприятия фото- и видеотехники, сотовых телефонов и т.п. Создание резервных копий. Видеонаблюдение.
Электронные чертежи и документация	Многофакторная аутентификация и авторизация пользователей. Использование специальных рабочих мест, не подключенных к сети и с физически заблокированными портами для работы с секретной и конфиденциальной документацией Отсутствие подключения к сети Интернет на рабочих местах. Физическая блокировка всех портов на рабочих местах. Регулярное создание резервных копий.
Линия сборки	Аутентификация и авторизация работников по пропуску.

	Запрет проноса на территорию предприятия фото- и видеотехники, сотовых телефонов и т.п. Видеонаблюдение. Отсутствие подключения к сети Интернет. Для разрешения потенциально опасных действий необходимо подтверждение минимум двух человек с расширенными полномочиями.
Сервер АСУ ТП	Многофакторная аутентификация и авторизация пользователей. Шифрование данных. Регулярное резервное копирование Регулярное обновление ПО Четкое разграничение прав у пользователей, использование подхода с минимально необходимыми правами. Логирование всех действий Защита сетевого периметра: файрволл, IDS/IPS. Создание honeypot.
Сервер отдела кадров	Многофакторная аутентификация и авторизация пользователей. Шифрование данных. Регулярное резервное копирование Регулярное обновление ПО Четкое разграничение прав у пользователей, использование подхода с минимально необходимыми правами. Логирование всех действий Защита сетевого периметра: файрволл, IDS/IPS.
Сервер мониторинга	Многофакторная аутентификация и авторизация пользователей. Регулярное обновление ПО Четкое разграничение прав у пользователей, использование подхода с минимально необходимыми правами. Защита сетевого периметра: файрволл, IDS/IPS. Создание honeypot.

Таблица 11.

Инф. ресурсы	Сценарии нарушителей	Обоснование достаточности мер
Бумажные чертежи и документация	Попытка кражи, копирования, подмены или порчи документов	Получить такую документацию можно только по пропуску и если есть специальное разрешение от СБ. Вся работа с секретными и конфиденциальными документами происходит в специально отведенных для этого комнатах под видеонаблюдением, на входе которых сидит охрана, поэтому пронести что-либо постороннее, а тем более вынести из такой комнаты не возможно. Запрет проноса на территорию предприятия фото- и видеотехники, сотовых телефонов исключает возможность копирования.

		К тому же есть видеонаблюдение. А от порчи спасает создание резервных копий.
Электронные чертежи и документация	Попытка кражи, копирования, подмены или порчи документов	Вся работа с секретными и конфиденциальными документами происходит в специально отведенных для этого комнатах на специально отведенных рабочих местах, не подключенных к сети, у которых физически заблокированы все порты. Доступ в эти комнаты возможен только по пропуску. Запрет проноса на территорию предприятия фото- и видеотехники, сотовых телефонов исключает возможность копирования. К тому же есть видеонаблюдение. От удаления данных спасает регулярное создание резервных копий
Линия сборки	Попытки сделать фотографии; попытки сломать	Допуск в помещения, в которых расположена линия сборки возможен только по пропуску. Запрет проноса на территорию предприятия фото- и видеотехники, сотовых телефонов исключает возможность сделать фотографии. Есть видеонаблюдение. К тому же для разрешения потенциально опасных действий необходимо подтверждение минимум двух человек с расширенными полномочиями – это означает, что в одиночку потенциально опасное действие с линией сборки не сделать.
Сервер АСУ ТП	Неавторизованный доступ к АСУ ТП	Многофакторная аутентификация пользователей означает, что даже при компрометации пароля в систему войти будет невозможно. Авторизация и использования принципа минимальных прав означает, что учетных записей с повышенными привилегиями будет очень мало. Регулярное обновление ПО означает, что в системе закрыты все известные уязвимости. Использование резервного копирования означает, что даже при порче данных, восстановление

		системы не займет много времени. Наличие защиты сетевого периметра означает, что неавторизованное подключение по сети будет крайне сложно реализовать. Наличие honeypot означает, что атакующий скорее всего попадет в ловушку и об попытке атаки будет известно СБ.
Сервер отдела кадров	Неавторизованный доступ к серверу, кража персональных данных.	Многофакторная аутентификация пользователей означает, что даже при компрометации пароля в систему войти будет невозможно. Авторизация и использования принципа минимальных прав означает, что учетных записей с повышенными привилегиями будет очень мало. Регулярное обновление ПО означает, что в системе закрыты все известные уязвимости. Использование резервного копирования означает, что даже при порче данных, восстановление системы не займет много времени. Наличие защиты сетевого периметра означает, что неавторизованное подключение по сети будет крайне сложно реализовать. Наличие honeypot означает, что атакующий скорее всего попадет в ловушку и об попытке атаки будет известно СБ.
Сервер мониторинга	Неавторизованный доступ к серверу, подменна данных.	Многофакторная аутентификация пользователей означает, что даже при компрометации пароля в систему войти будет невозможно. Авторизация и использования принципа минимальных прав означает, что учетных записей с повышенными привилегиями будет очень мало. Регулярное обновление ПО означает, что в системе закрыты все известные уязвимости. Наличие защиты сетевого периметра означает, что неавторизованное подключение по сети будет крайне сложно реализовать. Наличие honeypot означает, что атакующий скорее всего попадет в ловушку и

		об попытке атаки будет известно СБ.