|  |  |  |
| --- | --- | --- |
| Документ политики информационной безопасности | Существует ли политика информационной безопасности, которая одобрена руководством, публикуется и доводится до сведения всех сотрудников | да |
|  | Является ли он заявлением о приверженности руководства и определяет организационный подход к управлению информационной безопасностью. | да |
| Обзор и оценка |  |  |
|  | Имеет ли политику безопасности владелец, который несет ответственность за его обслуживание и проверку в соответствии с определенным процессом рассмотрения. | нет |
|  | Независимо от того, обеспечивает ли процесс проведение обзора в ответ на любые изменения, влияющие на исходную оценку, например: значительные инциденты с безопасностью, новые уязвимости или изменения в организационной или технической инфраструктуре. | да |

|  |  |  |
| --- | --- | --- |
| Форум по безопасности управленческой информации | Есть ли форум управления, чтобы обеспечить четкое руководство и видимую поддержку управления инициативами безопасности внутри организации | нет |
| Координация информационной безопасности | Существует ли межфункциональный форум представителей управления из соответствующих подразделений организации для координации внедрения элементов управления информационной безопасностью. | нет |
| Распределение обязанностей по информационной безопасности | Четко ли определены обязанности по защите отдельных активов и проведению конкретных процессов безопасности. | да |
| Процесс авторизации для объектов обработки информации | Существует ли процесс авторизации управления для любого нового средства обработки информации. Это должно включать все новые средства, такие как аппаратное и программное обеспечение. | да |
| Специалист по информационной безопасности | Независимо от того, получают ли консультации по информационной безопасности специалиста там, где это необходимо. | нет |
|  | Определенный индивидуум может быть идентифицирован для координации внутренних знаний и опыта для обеспечения согласованности и оказания помощи в принятии решений о безопасности | да |
| Сотрудничество между организациями | Были ли поддержаны надлежащие контакты с правоохранительными органами, регулирующими органами, поставщиками информационных услуг и операторами электросвязи для обеспечения быстрого принятия соответствующих мер и получения консультаций в случае инцидента с безопасностью. | да |
| Независимый обзор информационной безопасности | Независимо от того, осуществляется ли проверка политики безопасности на регулярной основе. Это делается для того, чтобы обеспечить уверенность в том, что организационная практика правильно отражает политику и что она возможна и эффективна. | нет |
| ***Безопасность доступа третьих сторон*** |  |  |
| Идентификация рисков от доступа третьих сторон | Требования безопасности в контрактах третьих | нет |
|  | Подтверждены ли типы доступа, классифицируются и причины доступа. | да |
|  | Были идентифицированы риски безопасности с сторонними подрядчиками, работающими на месте, и были реализованы соответствующие меры контроля. | нет |
| Требования безопасности в контрактах третьих лиц | Существует ли официальный контракт, содержащий или ссылающийся на все требования безопасности для обеспечения соответствия политикам и стандартам безопасности организации. | да |

|  |  |  |
| --- | --- | --- |
| **Физическая и экологическая безопасность** | | |
| ***Защищенная область*** |  |  |
| Периметр физической безопасности | Какое физическое устройство защиты границ было реализовано для защиты службы обработки информации. | коммутатор |
|  | Некоторыми примерами такого средства безопасности являются входные ворота для контроля карты, стены, укомплектованный прием и т. к. | да |
| Элементы управления физической записью | Какие существуют средства контроля доступа, позволяющие только уполномоченным персоналом работать в различных областях организации. | Приложения с идентификацией пользователя |
| Обеспечение офисов, помещений и помещений | Будут ли закрыты комнаты, в которых есть служба обработки информации, блокировки или сейфы. | да |
|  | Независимо от того, защищена ли служба обработки информации от стихийного и техногенного бедствия. | нет |
|  | Существует ли какая-либо потенциальная угроза со стороны соседних помещений. | нет |
| Работа в безопасных районах | Информация нужна только для понимания. Существует ли какой-либо контроль безопасности для третьих лиц или для персонала, работающего в безопасной зоне. | нет |
| Изолированные зоны доставки и погрузки | Независимо от того, изолированы ли область доставки и область обработки информации друг от друга, чтобы избежать любого несанкционированного доступа. | да |
|  | Была ли проведена оценка риска для определения безопасности в таких областях. | да |

|  |  |  |
| --- | --- | --- |
| ***Безопасность оборудования*** |  |  |
| Защита мест размещения оборудования | Было ли оборудование расположено в соответствующем месте, чтобы свести к минимуму ненужный доступ в рабочие зоны. | нет |
|  | Были ли изолированы элементы, требующие особой защиты, чтобы снизить общий уровень защиты. | нет |
|  | Были ли приняты меры по минимизации риска потенциальных угроз, таких как кража, пожар, взрывчатые вещества, дым, вода, дист, вибрация, химические воздействия, интерфейсы электропитания, электромагнитное излучение, наводнение. | да |
|  | Существует ли политика в отношении еды, питья и курения в непосредственной близости от служб обработки информации. | да |
|  | Наблюдается ли мониторинг состояния окружающей среды, что негативно скажется на средствах обработки информации. | да |
| Источники питания | Независимо от того, защищено ли оборудование от сбоев питания, используя постоянство источников питания, таких как несколько каналов питания, источник бесперебойного питания (ups), резервный генератор и т. д. | да, но не везде |
| Безопасность кабелей | Независимо от того, защищен ли кабель питания и телекоммуникационный кабель данными или вспомогательными информационными службами от перехвата или повреждения. | да |
|  | Существуют ли какие-либо дополнительные меры безопасности для чувствительной или критической информации. | нет |

|  |  |  |
| --- | --- | --- |
| ***Операционная процедура и обязанности*** |  |  |
| Документированные рабочие процедуры | Независимо от того, указала ли политика безопасности какие-либо рабочие процедуры, такие как резервное копирование, техническое обслуживание оборудования и т. | да |
|  | Будут ли такие процедуры документированы и использованы. | нет |
| Управление операционными изменениями | Независимо от того, подвергаются ли все программы, работающие на производственных системах, строгое управление изменениями, то есть любые изменения, которые должны быть внесены в эти производственные программы, должны пройти авторизацию управления изменениями. | да |
|  | Сохраняются ли журналы аудита для любых изменений, внесенных в производственные программы. | да |
| Процедуры управления инцидентами | Существует ли процедура управления инцидентами для борьбы с инцидентами с безопасностью. | нет |

|  |  |  |
| --- | --- | --- |
| *Требования безопасности систем* |  |  |
| Анализ и спецификации требований безопасности | Независимо от того, включены ли требования безопасности в состав требований бизнес-требований к новым системам или для улучшения существующих систем. | нет |
|  | Требования безопасности и идентифицированные элементы управления должны отражать ценность бизнеса в отношении задействованных информационных активов и последствия отказа от безопасности. | да |
|  | Проводится ли оценка рисков до начала разработки системы. | да |
| *Безопасность в прикладных системах* |  |  |
| Проверка входных данных | Независимо от того, проверены ли данные для системы приложений, чтобы убедиться, что они правильные и соответствующие. | да |
|  | Учитываются ли такие элементы управления, как: различные типы входов для проверки сообщений об ошибках, рассматриваются процедуры реагирования на ошибки проверки, определяющие обязанности всего персонала, вовлеченного в процесс ввода данных и т. Д. | да |
| Контроль внутренней обработки | Определяются ли области рисков в цикле обработки и включены проверки проверки. В некоторых случаях данные, которые были правильно введены, могут быть повреждены ошибками обработки или преднамеренными действиями. | да |
|  | Определены ли соответствующие средства управления для приложений для снижения рисков во время внутренней обработки. | да |
|  | Элементы управления будут зависеть от характера применения и влияния бизнеса на любую коррупцию данных. | да |
| Проверка подлинности сообщений | Была ли проведена оценка риска безопасности для определения необходимости проверки подлинности сообщения; и определить наиболее подходящий метод реализации, если это необходимо. | нет |
|  | Аутентификация сообщений - это метод, используемый для обнаружения несанкционированных изменений или повреждения содержимого передаваемого электронного сообщения. | нет |
| Проверка выходных данных | Независимо от того, проверен ли вывод данных прикладной системы для обеспечения правильности обработки хранимой информации и соответствия ее обстоятельствам. | да |
| *Криптографические средства управления* |  |  |
| Политика использования криптографических средств управления | Существует ли «Политика использования криптографических средств контроля для защиты информации». | нет |
|  | Была ли проведена оценка риска для определения уровня защиты, которую должна предоставлять информация. | да |
| Шифрование | Использовались ли методы шифрования для защиты данных. | да |
|  | Были ли проведены оценки для анализа чувствительности данных и необходимого уровня защиты. | да |

|  |  |  |
| --- | --- | --- |
| *Аспекты управления непрерывностью бизнеса* |  |  |
| Процесс управления непрерывностью бизнеса | Существует ли управляемый процесс для развития и поддержания непрерывности бизнеса во всей организации. | нет |
|  | Это может включать в себя план обеспечения непрерывности бизнеса Организации, регулярное тестирование и обновление плана, разработку и документирование стратегии непрерывности бизнеса и т. Д. | нет |
| Анализ непрерывности бизнеса и воздействия | Были отмечены события, которые могут вызвать перебои в бизнес-процессе: отказ оборудования, наводнение и пожар. | да |
|  | Была ли проведена оценка риска для определения воздействия таких перерывов. | да |
|  | Был ли разработан стратегический план на основе результатов оценки риска для определения общего подхода к непрерывности бизнеса. | да |
| Написание и реализация плана непрерывности | Были ли разработаны планы по восстановлению бизнес-операций в течение требуемого периода времени после прерывания или отказа от бизнес-процесса. | нет |
|  | Будет ли план регулярно проверяться и обновляться. | да |
| Рамки планирования непрерывности бизнеса | Существует ли единая структура плана непрерывности бизнеса. | да |
|  | Поддерживается ли эта основа для обеспечения согласованности всех планов и определения приоритетов для тестирования и обслуживания. | да |
|  | Определяет ли это условия для активации и лица, ответственные за выполнение каждого компонента плана. | нет |
| Тестирование, поддержание и переоценка плана непрерывности бизнеса | Регулярно проверяются ли планы обеспечения непрерывности бизнеса, чтобы они были актуальными и эффективными. | нет |
|  | Были ли продолжены планы обеспечения непрерывности бизнеса регулярными обзорами и обновлениями, чтобы обеспечить их постоянную эффективность. | нет |
|  | Были ли включены процедуры в рамках программы управления изменениями организаций, чтобы обеспечить надлежащее рассмотрение вопросов непрерывности бизнеса. | нет |

|  |  |  |
| --- | --- | --- |
| ***Соблюдение правовых требований*** |  |  |
| Определение действующего законодательства | Были ли четко определены и документированы все соответствующие нормативные, нормативные и контрактные требования для каждой информационной системы. | да |
|  | Были ли определены и документированы конкретные меры контроля и индивидуальные обязанности для удовлетворения этих требований. | да |
| Права интеллектуальной собственности (ПИС) | Существуют ли какие-либо процедуры для обеспечения соблюдения правовых ограничений на использование материалов, в отношении которых могут существовать права интеллектуальной собственности, такие как авторское право, права на дизайн, товарные знаки. | нет |
|  | Хорошо ли выполняются процедуры. | да |
|  | Независимо от того, поставляются ли проприетарные программные продукты в соответствии с лицензионным соглашением, которое ограничивает использование продуктов указанными машинами. Единственным исключением может быть создание собственных резервных копий программного обеспечения. | да |
| Охрана организационных записей | Независимо от того, защищены ли важные записи организации от разрушения убытков и функции фальсификаций. | нет |
| Защита данных и конфиденциальность личной информации | Существует ли структура управления и контроль для защиты данных и конфиденциальности личной информации. | да |
| Предотвращение злоупотребления средствами обработки информации | Независимо от того, рассматривается ли использование средств обработки информации для любых некоммерческих или несанкционированных целей, без одобрения руководства, рассматривается как ненадлежащее использование объекта . | нет |
|  | При входе в систему на экране компьютера отображается предупреждающее сообщение, указывающее, что введенная система является конфиденциальной и что несанкционированный доступ запрещен. | да |
| Регулирование криптографического контроля | Является ли регулирование криптографического контроля в соответствии с сектором и национальным соглашением. | нет |
| Сбор доказательств | Независимо от того, соответствует ли процесс сбора доказательств в соответствии с правовой и отраслевой практикой. | нет |
| ***Обзоры политики безопасности и технического соответствия*** |  |  |
| Соблюдение политики безопасности | Рассматриваются ли все области внутри организации для регулярного обзора для обеспечения соблюдения политики безопасности, стандартов и процедур. | да |
| Проверка технического соответствия | Регулярно проверялись ли информационные системы на соответствие стандартам обеспечения безопасности. | да |
|  | Независимо от того, осуществляется ли техническая проверка соответствия или под контролем компетентных, уполномоченных лиц. | нет |
| ***Вопросы системного аудита*** |  |  |
| Контроль системного аудита | Необходимо ли тщательно планировать и согласовывать требования аудита и действия, связанные с проверкой операционных систем, чтобы свести к минимуму риск сбоев в бизнес-процессе. | да |
| Защита средств системного аудита | Защищен ли доступ к инструментам системного аудита, таким как программное обеспечение или файлы данных, для предотвращения любого возможного злоупотребления или компрометации. | да |