sam solutions

ISO 27001: Система менеджмента информационной безопасности

Оглавление

Введение

Компания SaM Solutions является международным поставщиком услуг по разработке программных решений с более чем 25-летним опытом работы на рынке информационных технологий. Основные направления компании — разработка программного обеспечения под заказ на рынках США, Европы и СНГ, а также консалтинговые услуги в рамках процессов разработки. Вопросы безопасности и конфиденциальности информации являются одним из основных приоритетов компании, оправдывая высокий уровень доверия наших заказчиков, среди которых есть мировые лидеры в различных отраслях. В целях подтверждения соответствия законодательным требованиям Европейского Союза и требованиям заказчиков в сфере защиты информации руководство компании приняло решение внедрить **Систему Менеджмента Информационной Безопасности в соответствии со стандартом ISO 27001**. SaM Solutions успешно прошла сертификацию системы у престижного международного органа по сертификации TÜV Thüringen e.V.

Цель данного обзора ознакомить все заинтересованные стороны с общими аспектами информационной безопасности и защиты персональных данных со стороны SaM Solutions. Все перечисленные требования и меры задокументированы в качестве стандартов, политик и инструкций компании, а также доведены до всех сотрудников. Из соображений безопасности, в документе не описываются конкретные выполняемы процедуры, мероприятия и методы.

Область применения

Система Менеджмента Информационной Безопасности SaM Solutions выстроена по модели цикла Демминга **Plan—Do—Check—Act Cycle**, что полностью отвечает требованиям стандартов серии ISO и позволяет обеспечить развитие и эффективное функционирование системы.

Область действия системы включает в себя основной центр разработки в Республике Беларусь, а также штаб-квартиру в Германии, что позволяет обеспечить соответствие высоким требованиям защиты информации на всех этапах разработки программного обеспечения:

- ***RU: Проектирование, разработка и сопровождение программного обеспечения. Управление проектами и поставкой***

В область сертификации входят все процессы компании на всех этапах деятельности, в том числе процесс управления проектами, включая управление контрактами и поставкой.

Политики и Декларации

В целях определения стратегических аспектов деятельности и отношения к вопросам безопасности выработаны соответствующие политики по информационной безопасности и сделаны публичные декларации. Все документы размещены на официальном сайте SaM Solutions в открытом доступе.

Политика Системы Менеджмента Информационной Безопасности гласит следующее:

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных активов и данных, в том числе персональных данных физических лиц от нанесения им какого-либо ущерба посредством случайного или преднамеренного вмешательства в работу информационной системы организации или в случае возникновения инцидентов информационной безопасности.

При осуществлении своей деятельности в области сертификации ***«Проектирование, разработка и сопровождение программного обеспечения. Управление проектами и поставкой»*** компания SaM Solutions принимает на себя следующие обязательства:

- Соблюдать требования национального законодательства и применимого международного права, стандартов, нормативных правовых актов в области информационной безопасности.
- Не допускать несанкционированного или нецелевого использования информационных ресурсов и информационных систем.
- Использовать сертифицированное антивирусное ПО и избегать заражения вредоносными программами, расследовать все инциденты информационной безопасности.
- Использовать только лицензионное программное обеспечение в информационных системах организации.

- Классифицировать информацию, идентифицировать и оценивать активы, обнаруживать угрозы и уязвимости, управлять рисками, классифицировать объекты информатизации для обеспечения безопасности и отказоустойчивости информационной системы.
- Принимать эффективные меры для обеспечения целостности, доступности, конфиденциальности информации и данных, актуальности аппаратного и программного обеспечения для поддержания необходимого уровня безопасности информационной системы.
- Обеспечить непрерывность функционирования информационной системы, ее отказоустойчивость и быстрое восстановление в случае инцидентов информационной безопасности.
- Обеспечить постоянное совершенствование системы менеджмента информационной безопасности и соответствие требованиям, предъявляемым при сертификации.
- Поддерживать актуальность и доводить до контрагентов, третьих лиц и сотрудников политику системы менеджмента информационной безопасности.

Для достижения вышеуказанных обязательств и обеспечения результативного функционирования системы менеджмента информационной безопасности, руководство SaM Solutions гарантирует предоставление всех необходимых ресурсов.

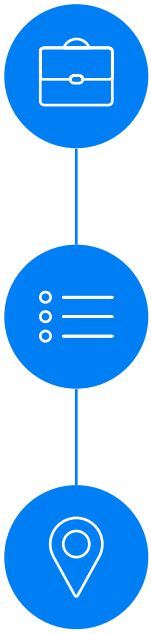
Помимо политики **Системы Менеджмента Информационной Безопасности**, в компании SaM Solutions принят еще ряд политик и сделаны декларации в области защиты информации и персональных данных:

1. **Политика защиты физических лиц при обработке персональных данных** — описывает цели, которые ставит перед собой SaM Solutions по защите персональных данных физических лиц, а также способы, которыми достигаются поставленные цели.
2. **Декларация обработки персональных данных** — описывает цели, характер и способы сбора и обработки персональных данных физических лиц со стороны компании.
3. **Политика информационной безопасности в отношении третьих лиц** — описывает взаимоотношения и требования, предъявляемые SaM Solutions к поставщикам и субподрядчикам.

Подробно с политиками можно ознакомиться на сайте SaM Solutions. Изданные документы позволяют прозрачно обозначить границы взаимодействия и ответственный подход компании к вопросам безопасности.

Управление Активами

Управление активами является одним из важнейших аспектов системного подхода при управлении безопасностью. SaM Solutions регулярно проводит инвентаризацию, учет и оценку активов. Общие управленческие решения по пересмотру категорий активов проводятся не реже одного раза в год. Менеджмент активов осуществляется с учетом всех требований стандартов серии ISO. На работников, которые осуществляют оборот чувствительной информации, возложена в том числе персональная ответственность за обеспечение ее безопасности. Выработанные системы категорирования и используемые методики основаны не только на ценности активов, но также учитывают аспекты безопасности активов относительно их иерархического уровня



БИЗНЕС УРОВЕНЬ

- **Взаимосвязь активов и их владельцев**
- **Влияние на бизнес-аспекты компании**

ПРИКЛАДНОЙ УРОВЕНЬ

- **Зависимость активов от их назначения и использования**
- **Группировка активов по категориям применимости и доступа**

ФИЗИЧЕСКИЙ УРОВЕНЬ

- **Взаимосвязь активов с их размещением**
- **Рассмотрение аспектов локализации активов**

Системный подход

Процесс принятия системных управленческих решений SaM Solutions в сфере информационной безопасности основан на **риск-ориентированном подходе.** Компания использует современные методы и модели управления рисками на всех этапах, планомерно выполняя каждый из них:

- Выявление риска и оценка вероятности его реализации и масштаба последствий, определение максимально возможного ущерба.
- Выбор методов и инструментов управления выявленным риском.
- Разработка риск-стратегии с целью снижения вероятности реализации риска и минимизации возможных негативных последствий.
- Реализация риск-стратегии.
- Оценка достигнутых результатов и корректировка риск-стратегии.

Руководство компании регулярно проводит анализ Системы Менеджмента Информационной Безопасности в соответствии с лучшими практиками и требованиями стандарта ISO 27001. Регулярно проводится анализ Системы Менеджмента Информационной Безопасности со стороны руководства. Проведение внутренних аудитов позволяет уточнить соблюдение установленных требований, а также провести верификацию принятых критериев оценки в системных аспектах.

К участию во внешних аудитах привлекается в том числе высший менеджмент компании, что обеспечивает вовлеченность руководства во все аспекты системного управления. Опыт, извлеченный из внутренних и внешних аудитов, лежит в основе модели постоянного совершенствования и формирует цели в области защиты информации на следующий отчетный период.

Физическая безопасность

Физическая безопасность, предусмотренная требованиями ISO 27001, обеспечивается с учетом современных технических требований. При этом для отдельных проектов и клиентов компания SaM Solutions организовывает дополнительные меры защиты, основанные на контрактных условиях, которые могут включать требования к периметрам защиты сверх тех, что внедрены и используется повседневно. Команды компании имеют опыт выполнения проектов с высокочувствительной информацией в условиях повышенных рисков и требований защиты.

В соответствии с требованиями ISO 27001 внедрены и используются следующие документированные защитные меры физической безопасности:

Допуск и контроль доступа

Компания обеспечивает высокий уровень контроля доступа и учет допуска лиц на территорию и в помещения. При этом обеспечивается процесс физической аутентификации и идентификации, а уровни допуска разбиты на категории.

Все периметры предприятия оборудованы системой видеонаблюдения с использованием архива видеозаписей и непосредственным наблюдением за информацией камер в реальном времени.

Доступ к периметрам осуществляется по электронным картам, которые обеспечивают процесс аутентификации с разграничением прав доступа.

Все помещения рабочих кабинетов закрываются на физические ключи, ведется централизованная выдача ключей с журналированием.

Двери рабочих кабинетов оснащены устройствами автоматического доведения закрытия с учетом противопожарных требований.

Должностные лица, осуществляющие оборот конфиденциальной информации, хранят ее в запирающихся шкафах и/или сейфах. Введены политики оборота информации с учетом использования устройств общего доступа (сетевые принтеры, сканнеры, факсы и т. д.).

Контроль мобильных устройств

Контроль за сменными носителями регламентирован соответствующими стандартами компании и включает в себя:

- ведение учета вноса/выноса техники и других устройств при входе в здания или на выходе;
- хранение носителей конфиденциальной информации отдельно и, при возможности, их маркировки специальным образом;
- ограничение использования подключаемых устройств там, где это целесообразно.

Охраняемые зоны

Охраняемые зоны являются помещениями с особым режимом доступа, разграниченные отдельными категориями допуска. К охраняемым зонам относятся серверные помещения, помещения, обслуживающие электропитание здания и другие помещения, классифицированные на основе анализа рисков. Физическая безопасность охраняемых зон обеспечивается соответствующими мероприятиями:

- Охраняемые зоны оборудованы внутренними системами видеонаблюдения.
- Доступ в охраняемые зоны возможен только с использованием ключа и электронной карты доступа, имеющей соответственно запрограммированную категорию допуска.
- Выдача ключей осуществляется строго идентифицированным работникам компании, имеющим соответствующую категорию допуска.

Безопасность операций

Документация Системы Менеджмента Информационной Безопасности включает в себя установленные процессы безопасности операций, которые обеспечивают в полной мере реализацию следующих требований:

- Использование только лицензионного программного обеспечения, своевременная установка всех обновлений, патчей и новых версий.
- Использование антивирусного программного обеспечения для обнаружения и борьбы с вредоносным программным обеспечением и кодом.
- Использование средств и систем резервного копирования для восстановления информации в случае нарушения свойств ее безопасности.
- Ведение логирования и учета событий и действий с использованием автоматизированной системы контроля доступности аппаратных и программных средств, наличия сбоев в их функционировании.
- Периодический контроль логов и событий, выполняемый вручную на определенном в соответствии с анализом рисков оборудовании и для определенного программного обеспечения.
- Централизованная установка программного обеспечения только уполномоченным персоналом.
- Проведение проверки безопасности устройств перед включением в рабочую среду после покупки, ремонта и иных случаев нахождения вне компании.

Контроль доступа

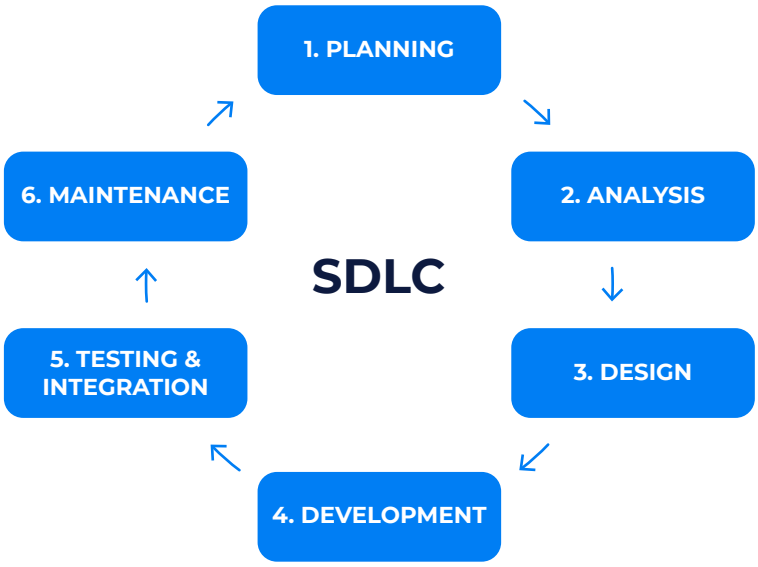
В рамках деятельности по обеспечению безопасности операций применяются специальные меры контроля доступа для обеспечения, соответствующего требованиям ISO 27001 уровня безопасности. Основные выполняемые требования включают:

- разграничение прав пользователей и их ролей как на уровне интрасети, так и в различных приложениях и системах, используемых компанией, таких как Jira, Confluence, Azure и другие;

- логирование и контроль действий пользователей для отдельных систем;
- настройки безопасности на уровне Active Directory, обеспечивающие необходимые настройки локальных устройств, такие как блокировка учетных записей при многократном вводе неверного пароля, блокировка системы по таймауту отсутствия действий пользователя и другие;
- ведение централизованного учета учетных записей и их блокировка в случае увольнения работника и/или переназначение прав в случае перевода работника в другое подразделение или на другой проект.

Введена и применяется политика чистого рабочего стола.

Приобретение, разработка и сопровождение систем



Выстроен и документирован Жизненный Цикл Разработки Программного Обеспечения, что позволяет на всех этапах четко определять роли и полномочия, обеспечивая безопасность как проектного окружения, так и обрабатываемой информации.

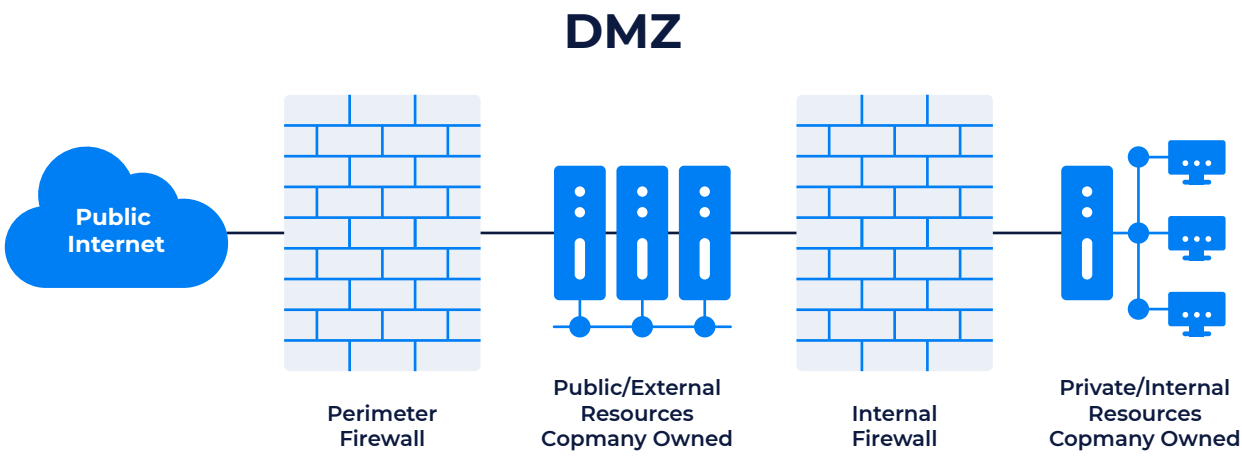
Все значительные изменения в проектное окружение и продакшн вносит авторизованный для этих действий персонал; соответственно, изменения в окружении, а также в программных пакетах дополнительно контролируются.

Тестирование безопасности разработки, а также уровень соответствия стандартам безопасности и набор защитных паттернов и средств определяются заказчиком.

Безопасность коммуникаций

В рамках **безопасности коммуникаций** разработана и поддерживается в актуальном состоянии схема сетей и коммуникаций. Применяется разделение систем и сетей, в том числе с установкой файрволлов между сегментами.

Создана **демилитаризованная зона (ДМЗ)**, в которую выносятся проекты и проектные сегменты, имеющие прямой доступ к сети Интернет. ДМЗ сегментирована и отделена от других сетей файрволлами, сегменты продакшн-окружения отделены от разработки и тестирования, которые также разделяются, если это возможно.



Введены ограничения на использование средств коммуникации между сотрудниками и для взаимодействия с заказчиками, что позволяет контролировать оборот конфиденциальной информации. Внутри компании используются определенные мессенджеры для общения, которыми централизованно управляет уполномоченный персонал.

Спектр коммуникаций и свойства определены специальным кодексом, который регламентирует устои корпоративной политики, стиль общения, а также характер и объем информации при ведении переговоров или рабочей деятельности.

Управление Инцидентами

Компания SaM Solutions задокументировала процедуры **управления инцидентами** с учетом классификации событий информационной безопасности. Разработаны меры и способы реагирования на события информационной безопасности начиная от мониторинга, заканчивая проведением расследований и мерами аварийного реагирования. Вся информация об инцидентах информационной безопасности сохраняется и используется для улучшения системы менеджмента информационной безопасности в целом и риск-менеджмента в частности.

В качестве мер превентивного реагирования на события информационной безопасности проводятся регулярные сканирования уязвимостей сетей и систем, а также пентесты.

Непрерывность бизнеса

Высокий уровень ответственности перед заказчиками является одним из приоритетов ведения бизнеса со стороны SaM Solutions. Компания разработала стратегию устойчивости к различным кризисным ситуациям в соответствии с которой вся инфраструктура компании может быть восстановлена полностью в течение 24 часов с момента полной ее гибели, например в случае природных катастроф или военных действий.

Для обеспечения отказоустойчивости применяются современные технологии виртуализации, резервного копирования данныхи другие разработки в области защиты информации. Резервные копии и отказоустойчивость периодически тестируются.

Соответствие

Обеспечение соответствия высоким требованиям в области защиты информации достигается путем регулярного анализа и системного подхода к безопасности, принятия мер реагирования, разработки корректирующих и предупреждающих действий и целей, анализа Системы Менеджмента Информационной Безопасности со стороны руководства. Верификация соответствия проводится в рамках внутреннего аудита.

Ежегодно, в целях подтверждения соответствия требованиям ISO 27001, SaM Solutions проходит внешний аудит со стороны международного органа по сертификации TÜV Thüringen e.V. Таким образом компания гарантирует наличие надзора третьей стороны по всем заявленным аспектам безопасности и принятым на себя обязательствам соответствия.

Выданные сертификаты с актуальной областью сертификации публично размещены на сайте компании **sam-solutions.com**.

SaM Solutions

Tel.: +375-17-3091709
Tel.: +49-8105-77890
www.sam-solutions.com

Data Protection Officer:

Alexandr Zorin
Chief Information Security Officer
E-mail: dpo@sam-solutions.com