127018, Москва, ул. Полковая 3
тел.: +7 (495) 777 95 82
info@seeneco.ru , www.seeneco.ru

Утверждаю _____

Генеральный Директор
ООО «Синеко-информационные системы»

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ

Версия 1.0

Дата: 06.05.2013

Содержание

Термины

Заключенная в круглые скобки часть термина может быть опущена при использовании.

Термин	Описание
Доступность	Состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно. *ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.*
Заказчик	Хозяйствующий субъект, потребляющий услуги по доступу к Программному обеспечению Исполнителя.
Информация	Сведения (сообщения, данные) независимо от формы их представления. *ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.*
Исполнитель	Общество с Ограниченной Ответственностью «Синеко – информационные системы».
Конфиденциальность	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. *ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.*
Материалы Заказчика	Все материалы, работы, данные, информация, которые были загружены, сохранены, обработаны или переданы в ходе использования Программного обеспечения Исполнителя от лица Заказчика, или любым пользователем, или приложением, или автоматизированной системой с использованием учетной записи Заказчика.
Программное обеспечение (Исполнителя)	Программное обеспечение, реализующее процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения информации под маркой Seeneco, которое принадлежит Исполнителю и доступно для Заказчика в режиме онлайнового доступа в соответствии с заключенным Договором.

Термин	Описание
	С точки зрения Законодательства РФ представляет собой совокупность баз данных, в которых содержится информация, и обеспечивающих ее обработку информационных технологий.
Объект	Пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа.
Субъект	Активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.
Целостность	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. *ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.*
ЦОД, Центр обработки данных	Специализированное здание для размещения серверного и коммуникационного оборудования. Центр обработки обладает всей необходимой для работы оборудования инженерной, телекоммуникационной и информационной инфраструктурой, включая программные и технические средства, системы контроля прилегающих территории и помещений. С точки зрения Законодательства РФ представляет собой совокупность информационных технологий и технических средств.

Сокращения

Сокращение	Расшифровка сокращения
РФ	Российская Федерация

1. Общие положения

1.1. Назначение документа

1.1.1. Настоящий документ (далее – Политика) определяет способы обеспечения необходимого и достаточного уровня защищенности Материалов Заказчика при использовании Заказчиком Программного обеспечения Исполнителя.

1.1.2. Политика представляет собой систематизированное изложение мер, методов и средств достижения информационной безопасности при использовании Заказчиком предоставляемых Исполнителем услуг и обеспечения конфиденциальности, целостности и доступности Материалов Заказчика.

1.2. Правовая основа документа

1.2.1 Законодательной основой Политики являются Конституция РФ, кодексы, законы, указы, постановления и другие нормативные документы действующего законодательства РФ, которые регулируют обеспечение информационной безопасности.

1.3. Доступность документа

1.3.1 Исполнитель обеспечивает свободный и неограниченный доступ к сведениям о реализуемых требованиях к защите Программного обеспечения и Материалов Заказчика.

2. Объекты и субъекты системы информационной безопасности

2.1. Основными объектами системы информационной безопасности являются:

- Программное обеспечение Исполнителя, предоставляемое Заказчику для использования;
- Материалы Заказчика;
- Инфраструктура ЦОД, используемая для развертывания Программного обеспечения Исполнителя.

2.2. Основными субъектами, участвующими в обеспечении информационной безопасности объектов защиты, являются:

- Заказчик, как собственник Материалов Заказчика;
- Авторизованные пользователи Заказчика, использующие Программное обеспечение в соответствии с возложенными на них функциями;
- Исполнитель, как собственник Программного обеспечения;

- Авторизованные сотрудники Исполнителя, выполняющие эксплуатационное обслуживание Программного обеспечения.

3. Цели защиты

3.1. Основной целью, на достижение которой направлены положения Политики, является защита Заказчика (как собственника Материалов Заказчика) и Исполнителя (как собственника Программного обеспечения) от возможного нанесения им ощутимого материального, физического или иного ущерба вследствие случайных или преднамеренных воздействий на Материалы Заказчика и Программное обеспечение Исполнителя.

3.2. Указанная цель достигается обеспечением и постоянным поддержанием следующих свойств Материалов Заказчика и Программного обеспечения:

- Конфиденциальность;
- Целостность;
- Доступность Материалов Заказчика и Программного обеспечения для Заказчика;
- Доступность Программного обеспечения для Исполнителя.

4. Меры, методы и средства обеспечения информационной безопасности

4.1. Технические средства защиты территории и помещений ЦОД

4.1.1. Уровень надежности ЦОД удовлетворяет требованиям, определенным международным стандартом TIA EIA 942 для уровня надежности Tier 3 или выше.

4.1.2. Здание ЦОД имеет укрепленные конструкции стен, дверей, окон.

4.1.3. Территория ЦОД удалена от трасс прохождения бытовых коммуникаций – воды, канализации, газа и т.п.

4.1.4. Здание ЦОД оборудовано следующими системами защиты:

- Посты круглосуточной охраны территории и внутренних помещений;
- Система контроля и управления доступом во внутренние помещения;
- Система охранной сигнализации;
- Система охранного телевидения;
- Система пожарной сигнализации и автоматического пожаротушения;
- Система бесперебойного и гарантированного электропитания;

- Система кондиционирования;
- Система основного и аварийного освещения;
- Круглосуточная служба мониторинга состояния всей инженерной инфраструктуры.

4.1.5. Телевизионные камеры системы охранного телевидения постоянно ведут наблюдение за следующими объектами:

- Прилегающая к зданию территория;
- Фасады и периметр здания;
- Помещения перед входом во внутренние части здания;
- Входы и выходы на лестничные клетки, коридоры;
- Входы в помещения постов охраны;
- Входы в помещения с серверным оборудованием.

4.1.6. Оборудование системы охранного телевидения обеспечивает:

- 24-часовую регистрацию изображений от всех телевизионных камер на устройствах цифровой видеозаписи;
- Хранение изображений от всех телевизионных камер не менее 1 (одного) месяца;
- Просмотр изображений от любой из телевизионных камер по выбору, по программе или по тревоге от охранной сигнализации;
- Ручное и аппаратное управление телевизионными камерами.

4.1.7. Телевизионные камеры наблюдения за внешним периметром здания имеют защиту от атмосферных осадков, пыли и изменений температуры.

4.1.8. Оборудование системы контроля и управления доступом обеспечивает:

- Интеграцию с системами охраны здания на программно-аппаратном уровне;
- Автоматизированный выпуск и учет персональных пропусков;
- Разграничение прав доступа персонала и посетителей в разные зоны здания;
- Организацию не менее 3 (трех) периметров доступа с возрастающей селективностью доступа – на входе в здание, на входе в помещения с серверным оборудованием, на входе в обеспечивающие помещения (пост круглосуточной охраны и т.д.);
- Вывод на экран информации о сотруднике и его фотографии в момент совершения прохода для оперативной сверки информации по карте с личностью проходящего
- Оперативную сверку личности с информацией пропуска (видеоверификацию) при проходе через турникет;
- Графическое отображение тревог, нештатных ситуаций, оперативной информации с выводом мест установки датчиков и считывателей;

- Регистрацию всех посещений здания сотрудниками и посетителями с указанием даты, времени посещения и иных данных;
- Формирование отчетов по журналу событий.

4.1.9. Входы во внутренние помещения ЦОД оборудованы электронными замками и считывателями карт, исключающими несанкционированное проникновение посторонних лиц.

4.1.10. Устанавливаемые в ЦОД средства и системы защиты имеют сертификаты соответствия требованиям нормативных документов.

4.2. Обеспечение работы оборудования ЦОД

4.2.1. Техническая инфраструктура ЦОД обеспечивает в помещениях с установленным оборудованием температурно-влажностный режим, соответствующий техническим условиям на используемые технические средства.

4.2.2. Сотрудники ЦОД обеспечивают содержания производственных площадей в соответствии с санитарно-гигиеническими правилами, правилами электрической и пожарной безопасности, установленными нормативно-правовыми актами РФ.

4.2.3. Для обеспечения круглосуточной работы оборудования сотрудники ЦОД в штатном порядке выполняют обслуживание оборудования, которое включает в себя проведение следующих мероприятий:

- Мониторинг производительности;
- Проведение резервного копирования;
- Переключение на резервные мощности;
- Переключение на резервные каналы связи;
- Проведение штатных процедур обслуживания и профилактических работ;
- Установка и обновление системного программного обеспечения оборудования;
- Модификация и замена оборудования.

4.3. Регламентация доступа в помещения ЦОД

4.3.1. Допуск сотрудников и посетителей во внутренние помещения здания ЦОД осуществляется в соответствии с установленными на территории ЦОД правилами пропускного и внутриобъектового режима.

4.3.2. Любые перемещения посетителей по зданию ЦОД происходят исключительно в сопровождении сотрудника ЦОД – дежурного инженера.

4.3.3. Сотрудникам и посетителям ЦОД запрещено проносить в помещения с установленным оборудованием любые опасные вещества (легковоспламеняющиеся, взрывоопасные и т.п.), любые пищевые продукты и напитки, а также прочие жидкости.

4.3.4. Внос оборудования во внутренние помещения ЦОД и вынос оборудования из помещений осуществляются исключительно с подписанием материальных пропусков на внос/вынос оборудования.

4.3.5. Сотрудники и посетители ЦОД соблюдают правила пропускного и внутриобъектового режима, установленные на территории ЦОД, а также санитарно-гигиенические правила, правила электрической и пожарной безопасности, установленные нормативно-правовыми актами РФ.

4.3.6. Доступ сотрудников или посетителей, нарушивших установленные на территории ЦОД правила режима, приостанавливается до устранения соответствующих нарушений.

4.4. Размещение Программного обеспечения в ЦОД

4.4.1. Программное обеспечение Исполнителя устанавливается на серверном оборудовании ЦОД с использованием терминального клиента.

4.4.2. Правила, установленные на территории ЦОД, запрещают сотрудникам и посетителям ЦОД совершать действия, которые могут причинить вред Программному обеспечению Исполнителя, Материалам Заказчика и оборудованию ЦОД, которое обеспечивает нормальное функционирование Программного обеспечения Исполнителя.

4.4.3. Серверное оборудование ЦОД, на котором установлено программное обеспечение Исполнителя, имеет защиту от подключения принтеров, внешних накопителей и других внешних устройств.

4.4.4. Технические и программные средства ЦОД обеспечивают защиту серверного оборудования, на котором установлено программное обеспечение Исполнителя, от несанкционированного и нерегистрируемого копирования данных, в том числе:

- С использованием отчуждаемых носителей информации;
- Мобильных устройств копирования и переноса информации;
- Коммуникационных портов и устройств ввода вывода, реализующих различные интерфейсы (включая беспроводные);
- Запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов);
- Устройств фото и видеосъемки.

4.4.5. В соответствии с внутренними правилами, сотрудники ЦОД не реже одного раза в год проводят сверку установленного в ЦОД оборудования.

4.5. Разграничение полномочий Заказчика и Исполнителя

4.5.1. На стадии ввода в действие Программного обеспечения Заказчик и Исполнитель выполняют настройки средств и механизмов обеспечения безопасности,

разграничивающие их права и не допускающие несанкционированного изменения предоставленных им полномочий.

4.5.2. Заказчик выполняет настройку контроля доступа субъектов в соответствии с ролями и ролевыми правами путем размещения заявок на администрирование Исполнителю.

4.5.3. Ответственные сотрудники Заказчика и Исполнителя выполняют контроль фактического состояния настроек ролей и ролевых прав на предмет их соответствия установленным правилам.

4.5.4. Сотрудники Заказчика являются единственными субъектами, которые имеют права и полномочия, необходимыми для:

- Использования Программного обеспечения Заказчика в своих бизнес операциях;
- Полного доступа к собственным Материалам, в том числе и к архивам Материалов.

4.5.5. Сотрудники Исполнителя являются единственными субъектами, которые имеют права и полномочия, необходимыми для:

- Эксплуатационного обслуживания Программного обеспечения (обновления версий, архивирования);
- Управления эталонными копиями (шаблонами) Программного обеспечения;
- Управления доступом Исполнителя к Программному обеспечению (возобновление, приостановление).

4.5.7. Определены следующие типовые роли:

- Пользователь Программного обеспечения (сотрудники Заказчика);
- Администратор Безопасности (сотрудники Заказчика);
- Администратор Программного обеспечения (сотрудники Заказчика);
- Администратор инфраструктуры и оборудования (сотрудники Исполнителя).

4.5.8. Исполнитель выполняет мониторинг работы Программного обеспечения, оборудования ЦОД, средств защиты при помощи системы мониторинга, предоставляемой ЦОД.

4.5.9. Заказчик самостоятельно принимает меры, необходимые и достаточные для выполнения собственными сотрудниками своих обязанностей и обеспечения безопасности Материалов Заказчика при работе с Программным обеспечением Исполнителя.

4.6. Регистрация событий в журналах

4.6.1. Информационная инфраструктура ЦОД выполняет регистрацию событий управления доступом и подключений к серверному оборудованию ЦОД в журналах регистрации событий с указанием следующих параметров:

- Создание и удаление учетных записей субъектов;
- Дата и время подключения и отключения;
- Идентификатор субъекта (логин), предъявленный при запросе доступа;
- Результат попытки входа: успешный или неуспешный (несанкционированный);
- Идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

4.6.2. Программное обеспечение Исполнителя выполняет регистрацию действий Авторизованных пользователей в журналах регистрации событий – в файлах и в базе данных.

4.6.3. Программное обеспечение не предоставляет Авторизованным пользователям средств модификации и уничтожения и информации, содержащейся в журналах регистрации событий.

4.6.4. Исполнитель обеспечивает сохранность и целостность журналов регистрации событий за счет обязательного архивирования журналов и перемещения в архивный каталог.

4.6.5. Создание архивов журналов регистрации событий выполняется в автоматическом режиме с периодичностью, согласованной между Заказчиком и Исполнителем. Архивы журналов регистрации событий перемещаются в архивный каталог.

4.6.6. Заказчик выполняет перенос архивов журналов регистрации событий с оборудования ЦОД на собственные носители информации. После выполнения переноса Заказчик выполняет удаление архивов журналов. Заказчик может привлекать Исполнителя к выполнению переноса и удаления архивов журналов.

4.6.7. Заказчик и Исполнитель используют информацию из журналов регистрации событий при анализе работы Программного обеспечения, при анализе причин нештатных ситуаций.

4.7. Обеспечение целостности

4.7.1. Исполнитель обеспечивает целостность Программного обеспечения за счет хранения эталонных копий Программного обеспечения – основной и резервной (резервных). Копии Программного обеспечения хранятся безопасно и независимо друг от друга.

4.7.2. При возникновении сбоев Программного обеспечения для восстановления используется основная копия. При выявлении повреждений основной копии, восстановление выполняется из резервной копии (резервных копий).

4.7.3. Исполнитель проводит учет внесения изменений в Программное обеспечение, связанных с установкой новых и обновлением существующих версий обеспечения.

4.7.4. Исполнитель обеспечивает целостность Материалов Заказчика за счет обязательного создания резервных копий. Резервному копированию подлежат:

- Материалы Заказчика;
- Журналы регистрации событий.

4.7.6. Создание резервных копий выполняется в автоматическом режиме с периодичностью и глубиной, согласованной между Заказчиком и Исполнителем.

4.7.7. Восстановление в случае нештатной ситуации Материалов Заказчика и Программного обеспечения из резервных копий выполняется в ходе совместной работы сотрудниками Заказчика и Исполнителя. Процедура восстановления регламентируется Исполнителем.

4.7.8. Защита Материалов Заказчика и Программного обеспечения Исполнителя от воздействий вредоносного кода выполняется средствами антивирусной защиты (Антивирусами).

4.8. Подключение к Программному обеспечению

4.8.1. К Авторизованным пользователям, которым разрешено подключение к Программному обеспечению, могут относиться исключительно сотрудники Заказчика и Исполнителя в соответствии с установленными им ролями.

4.8.2. Весь доступ к Программному обеспечению выполняется исключительно с использованием защищенного онлайнового канала взаимодействия.

4.8.5. Для блокирования несанкционированных подключений к Программному обеспечению используются установленные в ЦОД средства межсетевого экранирования (межсетевые экраны).

4.8.6. Межсетевой экран обеспечивает фильтрацию на сетевом уровне для каждого сетевого пакета независимо. Решение о фильтрации пакета с данными принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

4.8.7. Для защиты Программного обеспечения от сетевых атак, атак типа “отказ в обслуживании” на оборудование ЦОД используются сетевое оборудование и программные средства ЦОД.

4.8.8. В целях предотвращения несанкционированного доступа к Материалам Заказчика и Программному обеспечению посторонних лиц Исполнитель предоставляет механизм распознавания (аутентификации) каждого легального пользователя.

4.8.9. Для однозначной идентификации пользователя, при подключении к Программному обеспечению пользователь указывает назначенные ему параметры учетной записи – логин (уникальный идентификатор пользователя) и пароль подключения.

4.8.10. Каждый Авторизованный пользователь хранит параметры учетной записи для доступа к Программному обеспечению в секрете.

4.8.11. При компрометации (разглашении, распространении, утрате и т.п.) учетной записи Авторизованного пользователя, Заказчик немедленно уведомляет об этом Исполнителя. Исполнитель блокирует скомпрометированную учетную запись.

4.8.12. Используемый для аутентификации пароль учетной записи пользователя состоит не менее чем из 8 (восьми) буквенно-цифровых символов.

4.8.13. Количество последовательных неудачных попыток ввода пользователем пароля для аутентификации ограничивается 5(пятью) попытками. При превышении числа попыток, возможность дальнейшего ввода пароля блокируется.

4.8.14. Авторизованные сотрудники выполняют периодическую смену пароля. Срок действия пароля согласовывается между Заказчиком и Исполнителем. Максимальный срок действия пароля ограничивается 12 (двенадцатью) месяцами.

4.8.15. Заказчик обязан быть исключительно ответственным за обеспечение и поддержание своих сетевых соединений и телекоммуникаций, используемых для доступа к Программному обеспечению Исполнителя и влияющих на задержки, ошибки и возможные потери данных или их повреждения.

4.9. Использование Программного обеспечения

4.9.1. Исполнитель поставляет вместе с Программным обеспечением комплект документации, определяющий состав, назначение и порядок использования Программного обеспечения. Заказчик использует Программное обеспечение в соответствии с документацией.

4.9.2. Исполнитель контролирует использование Программного обеспечения Заказчиком. Аудит использования Заказчиком Программного обеспечения может быть проведен Исполнителем не чаще, чем один раз в квартал.

4.10. Завершение использования Программного обеспечения

4.10.1. По истечению срока действия Договора между Заказчиком и Исполнителем Исполнитель в согласованные сроки выполняет удаление Материалов Заказчика с оборудования ЦОД.

4.10.3. После завершения удаления Исполнитель выполняет очистку освобожденных областей памяти на носителях, ранее используемых для хранения Материалов Заказчика, средствами гарантированного стирания информации.