УТВЕРЖДАЮ

Генеральный директор ООО «Юсодент»

Рощин В. В. _____

г. Ярославль .

Система обеспечения информационной безопасности ООО «Юсодент»

Политика информационной безопасности

От 01 августа 2013 (в редакции от 09.12.2015)

Оглавление

Общие положения

Необходимость разработки Системы обеспечения информационной безопасности (СОИБ) обусловлена требованиями законодательства РФ и стремительным расширением сферы применения новейших информационных технологий и процессов в ООО «Юсодент», в том числе при обработке конфиденциальной информации.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованными лицам в нужное для них время.

Правовые основы построения СОИБ

Основой для построения СОИБ ООО «Юсодент» являются требования законодательства Российской Федерации, нормативные акты регулирующих органов, контрактные требования организации, а также условия ведения бизнеса, выраженные на основе идентификации активов организации, построения модели нарушителей и угроз.

Цели Политики информационной безопасности

Настоящая Политика Информационной Безопасности ООО «Юсодент» (далее – Политика) разработана в соответствии с целями и задачами обеспечения информационной безопасности, изложенными в Концепции Информационной Безопасности ООО «Юсодент» и основывается на требованиях законодательных и нормативных актов РФ в области безопасности информационных технологий и защиты информации, безопасности персональных данных.

Целью настоящей Политики является определение способов и форм обеспечения информационной безопасности ООО «Юсодент» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности.

Политика определяет необходимый и достаточный набор требований для разработки комплекса мер и процедур по обеспечению информационной безопасности в ООО «Юсодент», а также нормативных и методических документов, обеспечивающих ее

реализацию. Стоимость реализации применяемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

Область действия Политики

Положения настоящей Политики распространяются на всю конфиденциальную информацию ООО «Юсодент» (в т. ч. персональные данные) и ресурсы ее обработки. Требования настоящей Политики обязательны для всех: руководства, сотрудников (как постоянных, так и временных), а также третьих лиц, имеющих доступ к информационным ресурсам ООО «Юсодент» в рамках заключенных контрактов.

Порядок построения СОИБ

Для разработки эффективной Системы обеспечения информационной безопасности руководство организации должно знать, что защищать. Для этого необходимо определить все информационные активы (ресурсы), реализация угроз в отношении которых может нанести ущерб организации.

Разработка Системы обеспечения информационной безопасности начинается с проведения комплексного обследования объекта информатизации. По результатам обследования составляется ***Отчет о результатах проведения внутренней проверки***, который, наряду с законодательными и нормативными актами, служит основой для разработки следующих документов:

- Перечень информационных ресурсов, подлежащих защите;
- Модель угроз безопасности;
- Акт классификации информационной системы;
- Положение о разграничении прав доступа к обрабатываемым данным;

На основании этих документов формулируются конкретные требования по защите Информационной Системы ООО «Юсодент» (далее ИС) от утечки информации по техническим каналам и от несанкционированного доступа и осуществляется выбор организационных, программных, технических и т. д. мер и средств защиты информации, которые должны использоваться при эксплуатации ИС.

Используемые меры и средства защиты отражаются в Перечне реализуемых требований к защите конфиденциальной информации. Перечень реализуемых требований должен поддерживаться в актуальном состоянии. При изменении состава средств защиты или элементов ИС руководителем ООО «Юсодент» или лицом,

ответственным за обеспечение безопасности конфиденциальной информации, в него должны быть внесены соответствующие изменения.

Состав необходимых мер и средств защиты информации определяется с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

Требования к подсистемам

Система защиты должна включать в себя следующие подсистемы:

- подсистема управления доступом, регистрации и учета – управление доступом к информационным ресурсам ИС, управление парольной политикой, регистрация и учет действий пользователей ИС и процессов, регистрация действий администратора ИС;
- подсистема обеспечения целостности и доступности – контроль доступа в помещения ИС, обеспечение бесперебойной работы всех элементов ИС;
- подсистема антивирусной защиты – защита программного обеспечения и данных от вирусов и вредоносных программ;
- подсистема резервного копирования, восстановления и архивирования – резервное копирование и восстановление информации;
- подсистема доступа в Интернет – фильтрация сетевого трафика, защита ИС от несанкционированного доступа со стороны внешних злоумышленников;
- подсистема анализа защищенности;
- подсистема обнаружения вторжений;
- подсистема управления информационной безопасностью.

Детальные политики безопасности

Функционал каждой из подсистем ИС может быть описан одной или несколькими детальными политиками безопасности. Детальные политики безопасности являются неотъемлемой частью настоящей Политики. Детальные политики безопасности составляют коммерческую тайну ООО «Юсодент».

Актуальность Политики

Политика информационной безопасности должна оставаться актуальной и эффективной, поэтому ее положения должны пересматриваться не реже, чем один раз в три года, либо при изменении действующего законодательства и иных нормативных актов, а также в случае значительных изменений в ООО «Юсодент» (изменения структуры, стратегических целей бизнеса, актуальных угроз).

Ответственность пользователей

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ИС, неправомерный доступ, блокирование, модификацию информации, или нарушение работы ЭВМ и сетей (статьи 272, 273 и 274 УК РФ).

Ответственность пользователей ИС должна быть отражена в Положении о стоматологической клинике и должностных инструкциях сотрудников.