Организация многоуровневой защиты информации
и информационных каналов

Подсистема информационной безопасности ПК «Смета-Смарт».

Подсистема информационной безопасности позволяет разграничивать доступ как к функциям, так и к данным. Доступ к функции означает возможность или невозможность выполнить некое действие. Доступ к данным означает возможность или невозможность работать с определенными данными. Доступ к данным разграничивается как на уровне документов и справочников, так и на уровне учреждений. Например, можно настроить доступ пользователя только к определенному перечню документов конкретного учреждения или нескольких учреждений одной ЦБ. Таким образом ПК «Смета-Смарт» позволяет организовать рабочие места в ЦБ, где работа бухгалтеров разграничивается по учреждениям или по разделам бухгалтерского учета.

Подсистема позволяет настраивать безопасность как на уровне пользователя, так и на уровне ролей. Все события в системе фиксируются в журнале событий. По данным журнала событий можно получать специализированные отчеты о работе пользователей в системе.

Безопасность соединения.

Безопасность информационных каналов может быть обеспечена с помощью сертификатов, полученных в аккредитованном удостоверяющем центре. Если сертификат устанавливается на WEB-сервере, то подключение происходит по протоколу HTTPS, что обеспечивает шифрование трафика данных. Клиент Смарт позволяет подключаться по https протоколу с возможностью указания сертификата. Если в параметрах WEB-сервера установить настройки, требующие сертификат при подключении, то пользователь сможет подключиться только если укажет в Смарт-клиенте сертификат, предварительно полученный и установленный администратором на его компьютере. Ограничения подключений пользователей к серверу устанавливаются средствами настроек WEB-сервера и локальной сети.

Стоимость сертификата находится в районе 1 тыс. руб.

Выполнение требований безопасности по защите персональных данных, установленных законодательством РФ.

Если в информационной системе присутствуют персональные данные, то для такой системы должны выполняться требования законодательства РФ по защите персональных данных. Для обеспечения выполнения этих требований необходимо применение технических и организационных мер по защите информации, а также проведение аттестационных испытаний информационных систем на соответствие требованиям по защите персональных данных.

К техническим мерам относится применение сертифицированных программных и программно-аппаратных средств защиты информации.

К организационным мерам относится подготовка документов по защите персональных данных и их применение в организации .

Затраты ЦБ будут составлять порядка 1,5 - 2 млн. руб. и складываются из следующих основных частей:

Мероприятия	**Ориентировочная стоимость для ЦБ**
1. Технические мероприятия	
• с применением продуктов ViPNet для защиты канала связи	от 250 тыс. руб. за оборудование + 7800 руб. за каждое рабочее место.
• с применением продуктов Континент TLS для защиты канала связи	от 600 тыс. руб.
• с применением других средств защиты информации (СЗИ от НСД, АНЗ, антивирусы и пр.)	в зависимости от количества рабочих мест в ЦБ
2. Организационные мероприятия, всего: В том числе:	от 175 тыс. руб.
• поставка сервиса АльфаДок	55 тыс. руб.
• Аудит и разработка организационно-распорядительной и технической документации	от 120 тыс. руб
3. Аттестационные испытания	От 150 до 500 тыс. руб.

Примечание

Всю необходимую информацию по защите персональных данных вы можете получить в Кейсистемс-Безопасность http://www.npc-ksb.ru/