

# ВЫБОР ПОДХОДЯЩИХ МЕТОДОВ ЗАЩИТЫ

## ЗАВИСИТ ОТ ТОГО, ЧТО ЗАЩИЩАЕТСЯ И ОТ КАКИХ УГРОЗ

Об особенностях законодательства по защите персональной информации и мерах, которые должны предпринять компании, чтобы не попасть под санкции контролирующих органов, нам рассказал также руководитель отдела консалтинга и аудита компании Positive Technologies Сергей Гордейчик.

— **Какие основные методы защиты данных существуют сегодня?**

— Методов защиты существует очень много, и выбор подходящих зависит от того, что защищается и от каких угроз. Но если мы говорим о персональных данных, то государство в лице ФСТЭК и ФСБ определило минимальный набор механизмов защиты, который операторы должны реализовать. Прежде всего, от оператора требуется вынести информационные системы, обрабатывающие персональные данные, в отдельный сетевой сегмент, доступ к которому должен ограничиваться межсетевым экраном, а возможные сетевые атаки должны выявляться и блокироваться системами обнаружения и предотвращения вторжений. В дополнение к ним на серверах и рабочих станциях этих систем должны использоваться антивирусные средства. Внутри самой системы оператор должен реализовать адекватное разграничение доступа пользователей к данным, с тем чтобы каждый из пользователей получал ровно те сведения, которые действительно необходимы ему для выполнения своих служебных обязанностей. Кроме того, информационные системы должны генерировать данные аудита, необходимые для разбора возможных инцидентов. При передаче персональных данных по незащищенным каналам связи должны использоваться средства шифрования.

— **Что в плане технической защиты должны делать компании, на которые распространяется действие Закона «О персональных данных»?**

— Единого ответа на этот вопрос нет, поскольку тут регуляторы пошли по единственному правильному пути — дали оператору возможность выбирать адекватные меры защиты. Естественно, комплексы мероприятий по защите для поликлиники или бан-



• **Методические документы ФСТЭК и ФСБ не диктуют, какие именно средства защиты должны применяться. Оператору предоставлена возможность самостоятельно формулировать модель угроз, характерных для его информационных систем**

ковской системы, охватывающей всю страну, должны различаться. В одном случае достаточно стандартного набора средств защиты, таких как антивирус, фаервол, пароль. В других — требуются специализированные средства, включая системы шифрования и защиты от утечек по каналам побочного электромагнитного излучения. Основные требования к средствам защиты изложены в документах ФСТЭК и ФСБ. Для реализации сложных проектов логично привлекать специализированные компании, имеющие лицензии ФСТЭК и ФСБ и опыт построения информационных систем и их аттестации на соответствие требованиям 152 ФЗ «О персональных данных».

— **Насколько квалифицированные ИТ-специалисты должны рабо-**

**тать в компании, чтобы проблем с защитой персональных данных было минимум?**

— Поскольку вопрос соответствия 152 ФЗ «О персональных данных» — это далеко не только технический вопрос, то в его решение должны быть вовлечены все затрагиваемые подразделения: юристы, специалисты по работе с клиентами, ИТ- и ИБ-специалисты. Ничего принципиально нового требования регуляторов не привносят, все рекомендуемые процессы и средства защиты уже в том или ином виде присутствуют в большинстве компаний — соответственно, есть опыт их внедрения и обслуживания.

Требования к квалификации в значительной степени зависят от сложности системы. В одних случаях будет достаточно пользовательских навыков для эксплуатации системы в соответствии с разработанными инструкциями; в других, особенно если компания получает лицензии ФСТЭК, потребуются специалисты, которые имеют образование в области ИБ или прошли соответствующие курсы повышения квалификации.

— **Насколько велики должны быть вложения компании, чтобы ее оборудование для защиты персональных данных соответствовало требованиям законодательства?**

— Уровень расходов на приведение в соответствие требованиям 152 ФЗ «О персональных данных» и их поддержание в большой степени зависит от категории и объема обрабатываемой информации. Для небольших компаний — например, коллекторских агентств — для целей обработки ПД разумно выделить одно рабочее место, и в этом случае затраты будут исчисляться десятками тысяч рублей. При чем стоимость именно средств защиты в этом случае будет составлять 10–20%. Остальные расходы будут направлены на регламентацию организационных мероприятий, аттестацию и т. д. При масштабировании техническая составляющая затрат растет пропорционально сложности, а организационная — менее интенсивно. **IT**