О выборе межсетевого экрана для обеспечения защиты информационных систем персональных данных третьего и четвертого уровней защищенности

В соответствии с требованиями ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператору [персональных данных] необходимо использовать организационные меры и технические средства обеспечения безопасности персональных данных. В соответствии с п.13 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства РФ от 01.11.2012 № 1119) технические средства должны пройти процедуру оценки соответствия требованиям законодательства РФ в области защиты информации (сертификацию), в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. Определение актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных (далее - ИСПДн), может осуществляться оператором как самостоятельно, так и с привлечением компании-лицензиата ФСТЭК России путем обследования ИСПДн оператора, а также анализа применяемых в них мерах и средствах защиты информации.

При обработке персональных данных в ИСПДн операторами наиболее часто устанавливаются 3-й и 4-й уровни защищенности персональных данных. Также достаточно распространенным является полное или частичное размещение компонентов ИСПДн в центре обработки данных (далее - ЦОД), ресурсы которого предоставляются оператору ИСПДн со стороны владельца ЦОД на основании соответствующего возмездного договора.

Для нейтрализации актуальных угроз в отношении вышеуказанных ИСПДн, наряду с иными мерами безопасности, необходимо внедрение межсетевого экрана (далее - МЭ), выполняющего следующие задачи:

- контроль доступа (включая фильтрацию и контроль соединений) к серверам ИСПДн, размещенным в помещениях, принадлежащих оператору;
- контроль доступа (включая фильтрацию и контроль соединений) к серверам ИСПДн, размещенным в ЦОД;
- контроль межсетевого доступа к серверам и другим компонентам ИСПДн (включая автоматизированные рабочие места пользователей, на которых осуществляется обработка персональных данных), размещенным в помещениях, принадлежащих оператору;
-

контроль доступа к ресурсам сети «Интернет»;
- разграничение (контроль) доступа к категориям сетевых ресурсов, размещенным в ЦОД (web-серверы, базы данных, приложения и т.д.).

В соответствии с требованиями п.13 «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. приказом ФСТЭК России от 18.02.2013 № 21), а также принимая во внимание вышеописанный перечень задач, которые должны решаться МЭ, оператор для защиты ИСПДн 3-го и 4-го уровней защищенности должен использовать сертифицированные МЭ типа «Б» 6-го класса защиты (требования усиливаются от 6-го класса к 1-му), т.е. МЭ, реализующие следующие возможности:

- осуществление фильтрации сетевого трафика для отправителей информации, получателей информации и всех операций передачи контролируемой МЭ информации к узлам информационной системы и от них;
- обеспечение фильтрации для всех операций перемещения через МЭ информации к узлам информационной системы и от них;
- осуществление фильтрации, основанной на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия;
- осуществление явного разрешения или запрета информационного потока, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации, основанном на идентифицированных атрибутах;
- блокирование всех информационных потоков, проходящие через нефункционирующий или функционирующий некорректно МЭ;
- осуществление регистрации и учета выполнения проверок информации сетевого трафика и предоставление указанной информации уполномоченным администраторам;
- осуществление идентификации и аутентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;
- поддерживание определенных ролей по управлению МЭ;
- обеспечение перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному функционированию.

Перечень общепризнанных производителей МЭ, проведших в отношении своих продуктов процедуру оценки соответствия по требованиям законодательства РФ в области защиты информации (сертификацию), включает таких производителей как Fortinet, Checkpoint, Cisco. В настоящее время производитель Fortinet завершил сертификацию линейки моделей своих устройств (FortiGate) по требованиям к МЭ по 4-му классу защиты. Производитель CheckPoint собирается сертифицировать ряд актуальных моделей МЭ (предварительный срок сертификации - 2-й квартал 2017). Производитель Cisco также собирается сертифицировать ряд актуальных моделей МЭ (предполагаемый срок сертификации

на настоящий момент неизвестен).

МЭ всех производителей (Fortinet, CheckPoint и Cisco) полностью соответствуют функциональным требованиям регуляторов (ФСТЭК России). Если анализировать результаты проведения разных независимых тестирований можно сделать вывод, что по критерию качества МЭ вшеуказанных производителей примерно равны. На основании вышеописанного можно констатировать, что ключевыми критериями выбора МЭ являются:

1. пропускная способность с активными функциями FW, IPS и контроля приложений (NGFW);
2. стоимость внедрения и владения;
3. наличие сертификата соответствия требованиям законодательства РФ в области защиты информации.