Вопросы, связанные с применением Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, рассмотрены.

1. По вопросу отнесения инженеров-программистов (представителей оператора автоматизированных системах управления), разрабатывающих/дорабатывающих прикладное программное обеспечение для функционирования автоматизированной системы управления (мнемосхемы, алгоритмы программируемых логических контролеров и т. д.) к разработчикам программного обеспечения.

В соответствии с Квалификационным справочником должностей руководителей, специалистов и других служащих, утвержденным постановлением Минтруда России от 21 августа 1998 г. № 37, инженер-программист на основе анализа моделей и алгоритмов решения задач разрабатывает программы, обеспечивающие выполнение поставленной задачи, в том числе обеспечения безопасности информации, средствами вычислительной техники, проводит их тестирование и отладку.

В соответствии с пунктом 4 Требований указанные Требования предназначены для лиц, устанавливающих требования к защите информации в автоматизированных системах управления (заказчик), лиц, обеспечивающих эксплуатацию автоматизированных систем управления (оператор), а также лиц привлекаемых в соответствии с законодательством Российской Федерации к проведению работ по созданию (проектированию) автоматизированных систем управления и (или) их систем защиты (разработчик).

Таким образом к разработчикам системы защиты информации автоматизированной системы управления относятся в том числе инженеры-программисты, привлекаемые к разработке/доработке прикладного программного обеспечения для обеспечения безопасности информации в автоматизированной системе управления.

2. По вопросу использования анализаторов кода для выполнения мер по обеспечению безопасной разработки программного обеспечения.

Анализ кода в соответствии с мерами защиты информации по обеспечению безопасной разработки программного обеспечения может быть проведен с использованием автоматизированных средств или методом ручного анализа.

Выбор автоматизированных средств, применяемых для реализации мер защиты информации по обеспечению безопасной разработки программного

обеспечения, осуществляется оператором самостоятельно.

В случае отсутствия автоматизированных средств анализа кода, он может быть проведен методом ручного анализа.

3. По вопросу использования оператором автоматизированной системы управления программного обеспечения стороннего разработчика, который не выполняет мер защиты информации по обеспечению безопасной разработки программного обеспечения.

В соответствии с пунктом 13.4 Требований требования к мерам и средствам защиты информации, применяемым в автоматизированной системе управления, устанавливаются заказчиком на этапе формирования требований к защите информации в автоматизированной системе управления.

В процессе проектирования автоматизированной системы управления разработчиком должно быть выбрано программное обеспечение, соответствующее требованиям в части разработки программного обеспечения. В случае отсутствия возможности использования указанного программного обеспечения разработчиком системы защиты автоматизированной системы управления должны быть реализованы компенсирующие меры, связанные с применением недоверенного программного обеспечения, в соответствии с пунктом 22 Требований.

4. По выполнению требований к мерам обеспечения безопасной разработки, связанных с контролем принимаемых мер по выявлению, анализу и устранению уязвимостей программного обеспечения, осуществляемых заказчиком или оператором автоматизированной системы управления.

Контроль принимаемых мер защиты информации по выявлению, анализу и устранению уязвимостей, в том числе прикладного программного обеспечения сторонних разработчиков, может проводиться на этапе внедрения системы защиты автоматизированной системы управления при анализе уязвимостей автоматизированной системы управления в соответствии с пунктом 15.7 Требований.

Кроме того, при приобретении стороннего программного обеспечения необходимо предусмотреть процедуру запроса документов, подтверждающих тестирование программного обеспечения на уязвимости при разработке.