СКУД И СЕРТИФИКАЦИЯ ФСТЭК

П. Шмелев,
директор ЧОУ ДПО «Центр профессиональной подготовки»

Некоторое время назад у широкого круга заказчиков (потребителей) систем безопасности сложилось определенное убеждение о том, что системы контроля управления доступом (СКУД), выпускаемые в гражданский оборот на территории РФ, должны сопровождаться обязательным сертификатом ФСТЭК России на соответствие по требованиям безопасности информации. Логика такой точки зрения следующая. СКУД обрабатывает данные. В ряде случаев обрабатываемая информация относится к сведениям ограниченного доступа, безопасность которых должна быть обеспечена в силу закона (например, персональные данные). Следовательно, эта информация подлежит защите, а СКУД – обязательной сертификации в качестве средства защиты информации (СЗИ).
Цель настоящей статьи – объективное и всестороннее освещение комплекса вопросов, связанных с необходимостью и целесообразностью сертификации СКУД по требованиям безопасности информации как объекта гражданского оборота.

ЧАСТЬ 1. ПОДЛЕЖИТ ЛИ СКУД ОБЯЗАТЕЛЬНОЙ СЕРТИФИКАЦИИ?

Базовым нормативным документом, регулирующим правоотношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, оценке соответствия, является федеральный закон «О техническом регулировании» от 27.12.2002 № 184 (далее ФЗ-184). Этот закон также устанавливает права и обязанности участников этих правоотношений.

Обязательная сертификация является одной из форм обязательного подтверждения соответствия (ст. 20 ФЗ-184).

Сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров (ст. 2 ФЗ-184).

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента (ст. 23 ФЗ-184).

Технический регламент – документ, который принят международным договором Российской Федерации, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию, и устанавливает обязательные для применения и исполнения требования к объектам техничес-

кого регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации) (ст. 2 ФЗ-184).

Технический регламент должен содержать перечень и/или описание объектов технического регулирования, требования к этим объектам и правила их идентификации в целях применения технического регламента (ст. 7 ФЗ-184).

На дату написания статьи (май 2015) в Российской Федерации технические регламенты в отношении такого объекта технического регулирования, как «система контроля и управления доступом», не приняты.

В исполнение требований ФЗ-184 Правительством РФ принято Постановление от 01.12.2009 № 982 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии». В Перечне отсутствуют «средства управления доступом», «системы контроля и управления доступом».

Следует добавить, что ФЗ-184 устанавливает принципы технического регулирования. Одним из них является принцип недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов (ст. 19).

Таким образом, является очевидным следующее. Системы контроля и управления доступом – продукция, не являющаяся объектом технического регулирования, следовательно, СКУД не подлежит обязательной оценке соответствия в любых формах.

Однако этот вывод не раскрывает ответа на важный для производителей и потребителей СКУД вопрос: каким образом обеспечить надлежащую защиту информации ограниченного доступа, циркулирующей в СКУД?

ЧАСТЬ 2. СКУД И НАДЛЕЖАЩАЯ ЗАЩИТА ИНФОРМАЦИИ

Система контроля и управления доступом – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью («Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». ГОСТ Р 51241-2008). Цель применения СКУД – контроль доступа на объект в отношении субъектов доступа (людей, транспортных средств и т.п.) и/или управление таким доступом. Накапливаемая и обрабатываемая при этом информация может иметь различный уровень критичности. Почти всегда такая информация является «информацией с ограниченным доступом», в большинстве случаев это персональные данные.

Правоотношения, связанные с обработкой персональных данных (ПДн) регулируются федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ (ФЗ-152), а защита ПДн – нормативно-правовыми актами Правительства РФ, актами и руководящими документами (РД) ФСТЭК РФ, ФСБ РФ.

Практика показывает, что некоторые производители и службы эксплуатации СКУД, стремясь исполнить требования действующего законодательства в части обеспечения безопасности персональных данных, ошибочно ориентируются только на ГОСТ Р 51241-2008, полагая, вероятно, этот документ не только базовым в части технических требований к средствам и системам КУД, но и единственным в части требований по безопасности информации к ним.

Действительно, ГОСТ Р 51241-2008 требует обеспечить защиту информации от НСД (п. 5.1.7), устанавливает требования по защите программного обеспечения сетевых систем КУД от несанкционированного доступа (п. 5.5.7), а также требования по защите систем КУД с централизованным и универсальным управлением от несанкционированного доступа к информации (п. 5.5.8).

Однако важно понимать, что эти требования являются исчерпывающими лишь в целях настоящего ГОСТ, но не в целях исполнения иных нормативно-правовых актов РФ в части защиты информации. В этом контексте СКУД должна рассматриваться и как автоматизированная система, и как информационная система персональных данных.

Согласно РД ФСТЭК РФ «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Решение председателя Гостехкомиссии России от 30.03.1992) типовая СКУД в большинстве случаев должна быть классифицирована как многопользовательская АС, в которой одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности; не все пользователи имеют право доступа ко всей информации АС. Типовая СКУД, отнесенная к первой группе (в терминах данного РД) должна иметь класс защищенности 1Г. РД предъявляет к АС класса защищенности 1Г требования, реализуемые следующими подсистемами:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности.

В соответствии с Постановлением Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее ПП 1119) СКУД, обрабатывающая ПДн, должна рассматриваться как информационная система персональных данных (ИСПДн). В такой ИСПДн должен быть обеспечен 3 (реже – 2) уровень защищенности.

Приказ ФСЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее Приказ 21) устанавливает для 3 уровня защищенности более 40 мер по обеспечению безопасности, которые объединены в следующие группы:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- обеспечение целостности информационной системы и информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

Указанные меры реализуются путем создания системы защиты персональных данных (СЗПДн) СКУД. «СЗПДн включает в себя организационные и/или технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в информационных системах» (ПП 1119). Технические меры реализуются при помощи СЗИ.

К таким средствам относятся:

- СЗИ от несанкционированного доступа;
- антивирусное программное обеспечение;
- средства анализа защищенности;
- межсетевые экраны;
- средства обнаружения вторжений и пр.

Исчерпывающий состав СЗИ опре-

деляется исходя из актуальных угроз безопасности, определяемых на основе РД ФСТЭК:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Таким образом, СКУД со встроенным модулем защиты от НСД, отвечающем требованиям ГОСТ Р 51241-2008 (но не оснащенный иными СЗИ) не может обеспечить достаточный уровень защищенности ПДн. Такой модуль представляет собой лишь элемент комплекса мер, которые должны быть реализованы для обеспечения безопасности ПДн в ИСПДн СКУД.

Следует признать, что декларирование факта сертификации СКУД или системы КУД в качестве необходимых и достаточных мер защиты информации от НСД вводит потенциального потребителя такой продукции в заблуждение. Такой подход, в том числе и при продвижении СКУД как товара, не соответствует принципам объективности, которых следует придерживаться добросовестным участникам рынка.

Желание разработчиков «оснастить» продукт дополнительным документом (сертификатом) объяснимо, но как такая «псевдомодернизация» влияет на свойства СКУД и, в конечном счете, на задачи, решаемые СКУД?

ЧАСТЬ 3. ПОЧЕМУ СЕРТИФИКАЦИЯ СКУД КАК СЗИ ОТ НСД НЕ ВСЕГДА ЦЕЛЕСООБРАЗНА

Имеет право на существование следующая точка зрения на сертификацию СКУД как СЗИ от НСД: сертификация СКУД «замораживает» продукт, что препятствует его развитию. Эта точка зрения вытекает из соображений о необходимости постоянного обновления и модернизации продукта. Программное ядро СКУД, подвергаемое сертификации, после проведения процедуры сертификации не подлежит изменениям, а это не соответствует интересам потребителя.

СКУД как программный продукт подвержен более выраженной динамике, нежели СЗИ, в том числе и потому, что к СКУД предъявляются самые различные требования широким кругом потребителей, а требования к СЗИ зафиксированы лишь в документах ФСТЭК. Продолжительность жизненных циклов программных платформ СКУД и СЗИ различаются на порядок. По этой причине эволюция СКУД несовместима с интеграцией СЗИ в ядро СКУД, а в ряде случаев, и в компоненты средств КУД. Такую интеграцию, вызванную не соображениями об улучшении продукта, а лишь конъюнктурным стремлением придать продукту несуществующие качества нельзя считать разумным и профессиональным решением.

В большинстве случаев экономически целесообразным как для поставщика (инсталлятора), так и для потребителя (заказчика) СКУД является оснащение СКУД внешними сертифицированными СЗИ. Такой подход позволяет избежать избыточных затрат на «административное обслуживание» разрешительной документации, применять необходимые и достаточные внешние СЗИ к любой версии СКУД, обновлять программное обеспечение СКУД в ходе технической поддержки, существенно расширяя при этом спектр необходимых для потребителя параметров продукта и оптимизируя его стоимость. Напомним, что рядовое обновление «сертифицированного» СКУД до более старшей версии, изменение динамических библиотек, иные подобные действия, вносящие изменения в исходный код программного ядра, де-юре аннулируют сертификат соответствия СЗИ. Естественно, применяемые СЗИ должны пройти процедуру оценки соответствия (сертификацию).

Отдельно стоит упомянуть о практике сертификации «партии из 10 экземпляров» продукции. Закономерны следующие вопросы со стороны потребителя в адрес разработчика СКУД. Входят ли внедряемые ныне СКУД в эту партию? Указан ли в «Техническом паспорте АС» формуляр конкретного сертифицированного экземпляра СКУД? Соответствуют ли контрольные суммы исходных файлов внедряемого ПО СКУД контрольным суммам, зафиксированным в ходе сертификации?

Еще одним примером гибкости профессиональной этики некоторых разработчиков СКУД может служить и практика сертификации СКУД как СЗИ «по уровню контроля отсутствия НДВ» (недекларированных возможностей). Действительно, РД ФСТЭК РФ, установивший такие требования (1999), существует, следовательно, существует и сертификация на соответствие этим требованиям. Документ был предназначен, прежде всего, для обеспечения деятельности, направленной на противодействие иностранным техническим разведкам и на выявление т.н. программных закладок в программном обеспечении. Сертификация требует, помимо прочего, и наличия документации на ПО (к слову, требования к составу документации установлены рядом действующих ГОСТ СССР 1978-1979). При такой сертификации «оценке соответствия» может быть подвергнут программный модуль, не несущий никакой значимой функциональной нагрузки в части ЗИ, например, драйвер монитора. В то же время процесс сертификации по уровню контроля НДВ относительно недорог и обладает следующим важным качеством – приводит к появлению «Сертификата соответствия СКУД по требованиям безопасности информации». Однако стоит задуматься – оправданы ли затраты заказчиков СКУД, предпочитающих такой «сертифицированный» продукт и, следовательно, желающих гарантированно исключить наблюдение со стороны иностранных технических разведок за оттенками, например, серого цвета?

ЧАСТЬ 4. ЗИ В СКУД – ДОКУМЕНТАЛЬНОЕ ПОДТВЕРЖДЕНИЕ ВЫПОЛНЕННЫХ МЕР

Безусловно, наличия сертификатов соответствия даже нескольких СЗИ, которыми должен быть оснащен СКУД, недостаточно. Сертификат подтверждает лишь соответствие конкретного СЗИ одной группе неких требований (ГОСТ, ТУ, РД и т.п.), но не подтверждает соответствие установленным требованиям по ЗИ защищенной АС (или ИСПДн), каковой является СКУД в терминах регуляторов и контрольно-надзорных органов (например, Роскомнадзора РФ).

Оценка соответствия АС требованиям по ЗИ осуществляется в соответствии с нормативными актами регуляторов (ФСТЭК, ФСБ), руководящие документы которых заменяют технические регламенты (такие переходные положения предусмотрены ст. 46 ФЗ-184). В случае с АС оценка соответствия осуществляется в форме аттестации.

Аттестация объекта информатизации (АС, ИСПДн) по требованиям безопасности информации регламентируется Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными решением Коллегии Гостехкомиссии РФ № 7.2 от 02.03.2001. Этот документ не был опубликован, поэтому, де-юре, не наделен статусом нормативно-правового акта. С другой стороны, иного документа, исходящего от регулятора и формализующего алгоритмы оценки соответствия, ее результаты и документарное сопровождение этой работы, в настоящее время нет. Иная форма оценки соответствия автоматизированных систем требованиям по ЗИ – декларация соответствия – указа-

на в ФЗ-184, но действующим законодательством пока не регламентирована.

Проведение аттестационных испытаний предваряет разработка эксплуатационной документации системы защиты АС, в т.ч. технического паспорта. Технический паспорт содержит в себе информацию о составе технических средств и систем, входящих в состав АС, а также всех средств защиты информации.

Таким образом, аттестат соответствия удостоверяет, что АС соответствует требованиям нормативной документации по безопасности информации при соблюдении обеспечения условий функционирования АС и технологии обработки защищаемой информации, которые описаны в техническом паспорте. Аттестация не будет успешной, если СКУД будет оснащен только системой защиты от НСД (т.е. будет нейтрализована только одна из множества угроз безопасности). Органами, уполномоченными осуществлять аттестацию АС, являются лицензиаты ФСТЭК (лицензия на деятельность по технической защите конфиденциальной информации).

ЧАСТЬ 5. КТО ОБЯЗАН ВЫПОЛНЯТЬ МЕРЫ ПО ЗИ В СКУД?

Рассматривая меры по обеспечению безопасности ПДн в ИСПДн (в СКУД), следует обратиться и к положениям ФЗ-152. «Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных» (ст. 19).

«Безопасность персональных данных при их обработке в информационной системе персональных данных (далее – информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации. Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации» (Приказ 21).

Таким образом, защита информации в СКУД является обязанностью собственника (владельца) информационных ресурсов, а не обязанностью производителя каких-либо программно-технических средств.

ВЫВОДЫ

- СКУД не подлежит обязательной сертификации как средство защиты информации.
- Наличие любых сертификатов соответствия по требованиям ЗИ относительно СКУД создает лишь иллюзию защиты, не отражая реального состояния и эффективности мер защиты информации.
- Сертификация отдельных компонентов СКУД в качестве СЗИ в большинстве случаев экономически нецелесообразна. Эффективным является применение внешних специализированных СЗИ.
- Обязанность выбора и внедрения СЗИ лежит на собственнике информационных ресурсов.