ISSN 1680-2772

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ

№ 1

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ №1 (90) 2019

Научно-практический междисциплинарный журнал

Военная теория, военное строительство, стратегическое планирование и управление, вооружение и военная техника, системы контроля и испытаний

Отрасли наук: военные науки [военно – теоретические науки (20.01.00), военно – специальные науки (20. 02.00)].

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

Издается с ноября 1997 г.
Свидетельство о регистрации ПИ №77-3705 от 09.06.2000 г.
ISSN 1680-2772.

Выходит 4 раза в год.

Журнал включен в «Перечень ведущих периодических изданий» ВАК и систему РИНЦ

СОДЕРЖАНИЕ

УДК 004.056

© Сидак А.А., Василенко В.В.
© Sidak A., Vasilenko V.

ВЫРАБОТКА ОБЩИХ СТАНДАРТОВ, ОПРЕДЕЛЯЮЩИХ ТРЕБОВАНИЯ К ЗАЩИТЕ ДАННЫХ ПРИ ВЕДЕНИИ МЕЖГОСУДАРСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

DEVELOPMENT OF COMMON STANDARDS DETERMINING DATA PROTECTION REQUIREMENTS IN INTERSTATE ELECTRONIC DOCUMENT MANAGEMENT

Аннотация. *В статье освещены проблемные вопросы формирования требований к защите данных при создании общей цифровой платформы Российской Федерации и стран-партнеров, прежде всего в рамках Евразийского экономического союза. Предложены принципы выработки общих стандартов по защите данных, направленные на экономию средств и времени стран-участниц на создание доверительной межгосударственной цифровой среды и повышение эквифинальности систем электронного документооборота. Обоснован приоритет на адаптированное применение международных стандартов.*

Abstract. *The article highlights the problematic issues of forming data protection requirements when creating a common digital platform of the Russian Federation and partner countries, primarily within the Eurasian Economic Union. The principles of developing common standards for data protection aimed at saving finance and time of the participating countries on the creation of a trusting interstate digital environment and increasing the equifinality of electronic document management systems are proposed. The priority for the adapted using of international standards is justified.*

Ключевые слова*. Межгосударственное цифровое взаимодействие, электронный документооборот, цифровая платформа, цифровая экосистема, функциональное требование безопасности, профиль защиты, пакет требований, композиционность, эквифинальность, метастандарт.*

Key words. *Interstate digital interaction, electronic document management, digital platform, digital ecosystem, functional security requirement, security profile, requirement package, composition, equifinality, metastandard.*

В настоящее время отмечается глобализация процессов обработки данных и выход на наднациональный уровень. В целях обеспечения синергетического эффекта Председатель Правительства Российской Федерации М.В. Мишустин на форуме «Цифровое будущее глобальной экономики» (Алматы, 2020) призвал к совместному цифровому развитию стран Евразийского экономического союза (ЕАЭС). При этом им было отмечено, что весь электронный документооборот необходимо будет вести в доверительной универсальной межгосударственной среде, которая будет работать на общих стандартах. Очевидно, что подобные задачи актуальны и для других интеграционных объединений (Союзное государство, СНГ, ШОС, БРИКС и др.)

Возникает вопрос о том, как могут быть выработаны стандарты к защите данных, чтобы разные страны могли о них договориться как о единых.

Суверенный характер требований к защите данных обуславливает большую энтропию потенциальных единых стандартов, определяемую выражением

$H=\log\Omega$,

где Ω – число сочетаний значений факторов задания требований к защите данных, приводящих к соответствию требований и изделий информационных технологий (ИТ), их реализующих, единым стандартам.

Попытка снизить энтропию за счет конкретизации стандартов, разработанных в произвольной форме, может привести к длительной работе до достижения консенсуса. При этом консенсус между странами может быть и не достигнут.

Таким образом, для сближения позиций необходимо найти общую методологическую основу к зада-

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru;*
Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru.*

нию требований по защите данных.

В Российской Федерации в настоящее время имеется большой опыт по разработке национальных стандартов, нормативных правовых актов и методических документов в области защиты данных. Очевидно, что подобные шаги были предприняты и в других странах-партнерах. Если их проанализировать, то станет понятно, что все рассматриваемые страны так или иначе гармонизировали у себя соответствующие международные стандарты, определяющие функциональные требования безопасности (ФТБ) и требования доверия к безопасности.

Наиболее известна в этом отношении линейка стандартов ИСО/МЭК 15408/18045. В России действует уже их третья редакция [1-4].

Несмотря на некоторую сложность языка формализованного изложения и другие недостатки, ограничивающие в настоящее время применение в России, линейке стандартов ИСО/МЭК 15408/18045 свойственен ряд преимуществ [5]:

• четкое разделение требований безопасности на функциональные и требования доверия;

• постоянно развивающийся каталог идентифицированных шаблонов требований безопасности [2-3];

• наличие стандартизированных конструкций требований безопасности (профили защиты, задания по безопасности, пакеты требований), позволяющие унифицированно задавать требования безопасности, сопоставляя их с угрозами безопасности, целями защиты и спецификацией механизмов безопасности, реализующих эти требования;

• проработанность действий и шагов по оценке заданных требований безопасности [4].

Российский адаптированный перевод линейки стандартов ИСО/МЭК 15408 так или иначе используется и в других странах ЕАЭС и СНГ:

• в республике Казахстан – СТ РК ГОСТ Р ИСО/МЭК 15408, идентичный российскому ГОСТ Р ИСО/МЭК 15408;

• в республике Беларусь действуют СТБ.101.1-2014, СТБ.101.2-2014, СТБ.101.3-2014 на основе ИСО/МЭК 15408;

• в Азербайджанской республике стандарты AZS 356.1, AZS 356.2, AZS 356.3 на основе ИСО/МЭК 15408.

В России с использованием линейки стандартов ИСО/МЭК 15408/18045 в виде методических документов ФСТЭК России было разработано большое количество профилей защиты (ПЗ) для различных видов изделий ИТ [5]: операционных систем, межсетевых экранов, средств антивирусной защиты, средств доверенной загрузки, средств контроля съемных машинных носителей информации, систем обнаружения вторжений (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifi katsii/120-normativnye-dokumenty).

Использование профилей защиты позволило поднять на новый уровень процесс сертификации средств защиты информации по требованиям безопасности информации [5, 6]. Подробно вопросы применения профилей защиты в Российской Федерации рассмотрены в работе [5].

Профили защиты также активно разрабатывались и применялись для сертификации изделий ИТ и в других странах-партнерах России по интеграционным образованиям. Так, например, в Республике Беларусь профили защиты принимались в виде государственных стандартов: СТБ.101.11, СТБ.101.13 – ПЗ операционной системы, СТБ.101.14 – ПЗ маршрутизатора, СТБ.101.16 – ПЗ коммутатора.

Таким образом, очевидно, что в странах-партнерах, с которыми планируется создавать единую доверенную цифровую среду, имеется общая методологическая основа задания и оценки требований безопасности, предъявляемых к изделиям ИТ.

Вместе с тем, чтобы преодолеть недостатки линейки стандартов ИСО/МЭК 15408 и унифицировать критериальную базу задания требований безопасности, возможно будет целесообразным разработать единый стандарт в этой области. Это будет такой же метастандарт, который не определяет конкретные требования к изделиям ИТ, то есть не нарушает государственный суверенитет, но в то же время обеспечивает единые принципы задания требований и каталоги шаблонов требований. Для более широкой межгосударственной интеграции целесообразно, чтобы этот метастандарт был совместим с линейкой ИСО/МЭК 15408.

Как отмечалось выше, страны-партнеры имеют опыт в разработке профилей защиты. Конечно эти профили защиты у них разные. Таким образом, имея метастандарт, следующим шагом необходимо будет стандартизировать сами требования (функциональные и доверия), предъявляемые к изделиям ИТ, используемым для создания доверительной межгосударственной цифровой среды.

Для стандартизации требований безопасности на уровне профилей защиты можно использовать опыт создания международных технических сообществ (iTC), которые разрабатывают так называемые общие (или квалифицированные) профили защиты (cPP) [5].

Также конструктивным может оказаться не унификация ФТБ к комплексным изделиями ИТ, а стандартизация требований к отдельным компонентам и сервисам защиты данных для межгосударственного электронного документооборота.

Например, можно использовать следующие механизмы ИСО/МЭК 15408 [1, 3]:

• функциональные пакеты как промежуточную конструкцию ФТБ;

• разделение требований на требования к изделию ИТ и среде функционирования;

• разделение требований к базовому изделию ИТ и изделиям-компонентам.

При этом для меньших конструкций требований легче будет достичь консенсуса между странами-партнерами.

В дальнейшем можно будет применять механизмы метастандарта для композиции ФТБ при задании требований к комплексным изделиями ИТ в виде профилей защиты. При необходимости на этой основе могут разрабатываться семейства профилей защиты. В этом плане интересен опыт разработки документа ФСТЭК России «Руководство по формированию семейств профилей защиты» [7], в котором была заложена композиционность формирования требований безопасности на основе пакетов требований [5, 8]:

• определяется функциональный пакет для вида изделий ИТ;

• в рамках вида изделий ИТ выделяются типы;

• для каждого типа изделий ИТ также определяется функциональный пакет;

• для каждого класса защиты изделия ИТ определяется пакет доверия;

• при формировании профиля защиты для конкретного типа изделия ИТ в него включаются функциональные пакеты вида и типа изделий ИТ, а также пакет доверия, соответствующий классу защиты изделия ИТ.

Следующий уровень проблемы – стандартизация средств защиты информации и средств обеспечения безопасности информационных технологий. Даже, если ФТБ к изделию ИТ будут единые, эти изделия будут разрабатываться и оцениваться по-разному в соответствии с внутренними процедурами конкретной страны. В целях признания странами-партнерами результатов оценки изделий ИТ для применения в межгосударственных системах электронного документооборота может быть выработано соглашение, в чем-то похожее на международное соглашение CCRA (https://www.commoncriteriaportal.org/ccra/).

Следующая проблема – совместимость изделий ИТ, применяемых в разных национальных сегментах единой системы межгосударственного электронного документооборота. Изделия ИТ разных стран могут соответствовать единым требованиям безопасности, но не быть совместимыми между собой. Прежде всего такая совместимость необходима по функциям управления и регистрации событий безопасности.

В этом направлении представляет интерес ИСО/МЭК 15408-2 [2], в каталоге которого для каждого компонента ФТБ предусмотрены действия по управлению (атрибутами, функциями безопасности и их данными) изделий ИТ, а также события безопасности и данные, подлежащие регистрации (дифференцированы по уровням аудита).

Следующий шаг в этом направлении был сделан в рамках рабочей группы (РГ) технического комитета по стандартизации «Защита информации» (ТК 362) – подготовлен проект национального стандарта ГОСТ Р «Защита информации. Регистрация событий безопасности Требования к составу регистрируемой информации», который определил требования к составу и содержанию регистрируемой информации для различных типов событий безопасности. Указанный стандарт (после его принятия) может быть рекомендован для применения на межгосударственном уровне по отношению к системам межгосударственного электронного документооборота.

Унификация регистрации событий безопасности создает основу для внедрения единых систем мониторинга и реагирования на инциденты информационной безопасности. Общая схема, уровни и принципы построения систем мониторинга и управления инцидентами информационной безопасности рассмотрены в работе [9]; требования к уровням мониторинга определены в проекте национального стандарта ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения», разработанном в рамках РГ ТК 362.

Технически положения проектов стандартов по регистрации и мониторингу ИБ, а также функционал по управлению инцидентами ИБ может быть реализован применением линейки изделий типа Neurodat, хорошо зарекомендовавших себя в самых масштабных ИТ-инфраструктурах с большой номенклатурой разнородных цифровых платформ и изделий ИТ.

Таким образом, реализация предложенного в настоящей статье подхода позволит в приемлемые сроки выработать общие для ЕАЭС (и других интеграционных образований) стандарты по защите данных, повысить уровень эквивалентности и сервисности межгосударственного цифрового взаимодействия, встроить системы межгосударственного электронного документооборота в цифровые экосистемы стран-участниц.

Литература

1. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2014.

2. ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. М.: Стандартинформ, 2014.

3. ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. М.: Стандартинформ, 2014.

4. ГОСТ Р ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. М.: Стандартинформ, 2014.

5. Сидак А.А. Вопросы применения профилей защиты // Двойные технологии. 2019. № 2. – С. 88-91.

6. Сидак А.А. Особенности сертификации продуктов и ИТ-систем на основе Общих критериев // Защита информации. Инсайд. 2005. № 4. – С. 51-53.

7. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003: [Электронный ресурс] // ФСТЭК России, 2019. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/401-

rukovodyashchijdokument-gostekhkomissiya-rossii-2003-god2 (Дата обращения: 21.01.2020).
8. Сидак А.А. Композиционный подход к формированию требований к изделиям, реализующим функции безопасности в информационных системах. Семейства профилей защиты// Стратегическая стабильность. 2013. № 3. – С.40-42.
9. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных Систем мониторинга и реагирования на инциденты информационной безопасности// Стратегическая стабильность. 2018. № 1. – С.64-67.

Материал поступил в редакцию 14.02.2020 г.