Кибербезопасность – новое понятие или хорошо известное настоящее?

И.И. Лившиц, А.В. Неклюдов (СПИИРАН)

В номере журнала, посвященном теме кибербезопасности логично будет внести определенность с генезисом этого модного сегодня понятия, что будет, безусловно, полезно для понимания изучаемой проблемы и позволит в дискуссии о предмете оперировать измеряемыми величинами.

Поскольку в России все, что связано с информационными технологиями (ИТ), в значительной степени зависимо от зарубежных центров компетенции в области высоких технологий, логично будет предпринять попытку поиска истоков кибербезопасности в одном из них. Обратившись к информационным ресурсам National Institute of Standards and Technology (NIST)[1], обнаружим упоминание о документе «Preliminary Cybersecurity Framework» с датой публикации 28 февраля 2013 г., разработанном во исполнение документа «Executive Order 13636». То есть на момент публикации настоящей статьи проблематика кибербезопасности в США имеет историю длительностью уже более пяти лет и не может считаться неведомой темой для всего мыслящего прогрессивного человечества.

Ключевые слова: стандарты, кибербезопасность, оценка, общие критерии, информационные технологии.

Введение

Рассмотрим упомянутый документ «Preliminary Cybersecurity Framework» и постараемся оценить, является ли он каким-то новым словом в области безопасности ИТ? Отнюдь нет. Свидетельством тому является Приложение «Appendix A. Framework Core», в котором в соответствие с позициями, указанными в «Preliminary Cybersecurity Framework», рассматриваются конкретные документы с историей, гораздо большей пяти лет. Появление этих документов никоим образом не связано с проблематикой кибербезопасности, например, ISO/IEC 27001 (первая версия вышла в 2005 г., а вторая версия в 2013 г.) [1] и NIST SP 800-53 Rev. 4.

Отсюда можно сделать вывод, что кибербезопасность является только лишь новым брендом, создатели которого даже и не пытались наполнить какими-то новыми смыслами, а сразу увязали подходы к обеспечению кибербезопасности с положениями проверенных временем документов по безопасности ИТ. Почему же так произошло, спросит читатель? Потому, что это находится полностью в русле современных подходов ведения дел на планете Земля. Зачем просто пользоваться проверенными старыми вещами, если можно их постоянно «заворачивать в новые обертки» и выдавать за «инновационный» продукт. Все «эффективные менеджеры» и прочие креативные индивидуумы сразу получаются при деле, минимум затрат, максимум отдачи, а поскольку наполнение «новых оберток» смыслом, в свою очередь, перекладывается на плечи центров компетенции, то и риски минимальны.

Существующие зарубежные документы

Между тем документы, содержащие и смысл, и внятные механизмы, имеют долгую и знаменательную историю. Так, документ «SP 800-53 Rev. 4. Security and Privacy Controls for Federal Information Systems and Organizations», входящий в состав «Risk Management Framework» (RMF), фактически ведет свою «родословную» от программы «DoD Computer Security Initiative Program», (DoD CSIP), стартовавшей еще в далеком 1978 г. Да и документ «ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements» хотя и не является прямым потомком DoD CSIP, но своим появлением также обязан хорошо известным британским инициативам из 80-х годов XX века.

DoD CSIP — тема отдельного большого разговора, поэтому мы акцентируем внимание читателей только на одном факте — тогда, в 1978 г. министерство обороны США инициировало программу, целью которой являлось достижение такого порядка вещей, при котором потребителям были бы широко доступны продукты ИТ, обладающие функциональностью, соответствующей единым требованиям безопасности и подтвержденной оценкой в независимой авторизованной лаборатории. DoD CSIP достигал своей цели, что и было зафиксировано в «Federal Information Security Management Act of 2002 (Public Law 107-347 Title III)» в виде указания на создание RMF.

Таким образом, даже в США, имеющих в своей юрисдикции центры компетенции в области ИТ уровня NIST, не все оптимально. В результате носи-

[1] https://www.nist.gov/node/1310901/archived-documents

тели смыслов в области ИТ вынуждены приводить к некому разумному знаменателю инициативы создателей новых брендов. И надо сказать, что случай с «Cybersecurity Framework» отнюдь не уникален.

Состояние кибербезопасности в России

А как дела с кибербезопасностью обстоят в России? Откровенно говоря — неважно, к сожалению... Дело в том, что в условиях отсутствия в России центров компетенции в области ИТ с подачи органов, регулирующих вопросы безопасности области ИТ, были сформированы две ложные посылки. Посылка первая — информационная безопасность (ИБ) существует отдельно от ИТ. Посылка вторая — для различных видов информации необходимы различные подходы к защите информации.

Первая посылка опровергается всем мировым опытом. Все значимые производители продуктов ИТ на мировом рынке не отделяют вопросы ИБ от ИТ. Есть ряд производителей, которые позиционируют себя исключительно как разработчики решений по ИБ, но по факту это либо продукты ИТ, в которых функциональность безопасности чрезмерно разрекламирована, либо специализированные продукты, которые устанавливаются в среду функционирования, уже имеющую систему безопасности. При очень сильном желании продукт ИТ без функций безопасности, конечно, получить можно, но для этого надо будет приложить достаточно усилий, вплоть до его создания именно в таком «чистом» виде, без функций безопасности.

На рынке имеется достаточное число продуктов ИТ, функциональность безопасности которых уже оценена независимыми авторизованными лабораториями. Понятно, что есть проблема доверия к функциям безопасности продукта ИТ, разработанного или прошедшего оценку соответствия в другой юрисдикции. Но отсутствие функции безопасности и отсутствие достаточного доверия к функции безопасности из другой юрисдикции — это, согласитесь, две большие разницы. Кстати, тот же NIST не разделяет ИТ и вопросы их безопасности, о чем свидетельствует нахождение «Computer Security Division» в составе «Information Technology Laboratory».

Вторая посылка также опровергается всем мировым опытом. Документ «Common Criteria for Information Technology Security Evaluation», его реплика в виде международного стандарта «ISO/IEC 15408. Information technology. Security techniques. Evaluation criteria for IT security» (равно как и ГОСТ Р ИСО/МЭК 15408) [2–4], стандарт «ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements» (равно как и ГОСТ Р ИСО/МЭК 27001), RMF предусматривают единые требования для любых видов информации. Напомним, что любое цифровое устройство может рассматриваться как конечный автомат (КА), который обрабатывает информацию, распознавая выражения, составленные из слов, заданных над определенным алфавитом [6]. Поскольку практически все современные продукты ИТ опираются на двоичную систему счисления, то значит и элементарный алфавит соответствующего КА тоже будет двоичный. Понятно, что можно определить другие типы алфавитов конечного автомата, слова над ними и правила построения выражений. Так в реальности и делается, но многие вопросы как общего технологического плана, так и безопасности решаются именно на уровне элементарного алфавита — двоичного. А биты — они всегда просто биты, если, конечно, не принять дополнительных мер по снабжению их соответствующими атрибутами. Биты персональных данных и биты государственных информационных систем неотличимы друг от друга [5]. Выскажем даже совершенно крамольную вещь — биты информационного потока, содержащего сведения, составляющие государственную тайну, также неотличимы от прочих битов.

Поэтому применительно к КА главная задача защиты информации звучит так — настроить функциональность КА таким образом, чтобы обеспечить различимость битов различных информационных потоков в конкретной среде и обеспечить на этой основе их изоляцию в процессе обработки. Сколько для этого потребуется определять типов алфавитов и слов над ними — это отдельный вопрос. Но не подлежит сомнению, что многие вопросы безопасности будут решаться на уровне элементарного алфавита — двоичного.

Организационные вопросы кибербезопасности

Перейдем к организационным вопросам, а именно, к основным органам исполнительной власти, регулирующим в России вопросы обеспечения ИБ.

Федеральная служба безопасности РФ (ФСБ России) в части вопросов обеспечения ИБ в гражданском секторе может быть условно представлена в виде системы, состоящей из администраторов, инженеров и математиков. Именно наличие в составе системы достаточно квалифицированных инженеров и математиков (внутренняя оппозиция) создают противовес безграничному полету фантазии администраторов и спасают ее (систему) от полного провала. Эта система инициативы проявляет мало, и в целом не в полной мере адекватна современному уровню развития ИТ. В выступлениях представителей ФСБ России на отраслевых форумах триединая сущность службы достаточно хорошо проявляется[2].

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) представляется монолитной системой без внутренних сдержек и противовесов. ФСТЭК России широко знаменита тем, что практически не отменяет свои нормативные документы. Абсолютное большинство нормативных документов созданы под впечатлением от зарубежных регламентов, глубоко понять которые ФСТЭК Рос-

[2] https://www.securitylab.ru/blog/personal/valerykomarov/343982.php

сии оказалась не в состоянии. В то же время результат попыток ФСТЭК России создать что-то собственными силами не был принят даже на уровне экспертизы Минюста (классический пример — 4 тома КСИИ). ФСТЭК России создает нормативные документы низкого качества, например, полагая возможным наличие для каждого типа информации собственного «уникального» набора мер защиты. Четырежды переводилось приложение «Appendix D. Security control baselines — summary» из документа NIST SP 800-53, и все четыре перевода отличаются и друг от друга, и от первоисточника, а смысл NIST SP 800-53 при переводе полностью утрачен. Чувство меры ФСТЭК России несвойственно, и взяв за основу для сертификации средств защиты ГОСТ Р 15408 (идентичен ISO/IEC 15408) служба создала явно избыточное число профилей защиты (более 20), в которых недостатки зачастую видны даже при беглом чтении. Для аналогичных целей за рубежом для одного направления создается только один профиль защиты, но выверенный до предела. На отраслевых форумах представители ФСТЭК России выступают мало, дают абстрактные ответы и предлагают «писать письма» (например, по спорным вопросам ФЗ-187 КИИ)[3].

Касательно российских нормативных документов на традиционные русские вопросы «Кто виноват?» и «Что делать?» авторы могут дать очень простые и, к сожалению, неприятные ответы. Виноваты мы все. И те, кто разрабатывал неадекватные нормативные документы, преисполненный собственной значимости, и те, кто соблюдал эти же неадекватные нормативные документы, тая надежду на «индульгенцию». Что делать? Нужно просто перестать заниматься насилием над здравым смыслом и «успешным обеспечением безопасности», а сосредоточиться на правильном и эффективном применении всего двух документов, на которых сегодня зиждется вся безопасность ИТ — «Common Criteria for Information Technology Security Evaluation» или его реплики — серии ISO/IEC 15408 и ISO/IEC 27001. Тем более, что в России есть идентичные международным национальные стандарты — ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 27001.

В качестве рекомендаций для смягчения текущей ситуации с нормативными документами ФСТЭК можно отменить отраслевые инициативы (например, инициативы по созданию центров компетенции ИБ на базе Сбербанка[4], создание отраслевых альянсов в области ИБ по инициативе «Норильского Никеля»[5] и пр.), которые основаны на глубокой предметной экспертизе, наличии квалифицированных кадров, достаточных ресурсах и главное — на желании повышать степень безопасности своих ИТ в предельно сжатые сроки. Этот пример отраслевого взаимодействия в определенной мере повторяет путь, пройденный в 80-х г. XX века нашими «западными партнерами». В то же время различные международные сообщества постепенно «выводят из оборота» собственные системы оценки и применяют далее только наилучшие международные стандарты ИСО и ИСО/МЭК серий 15408, 15504, 20000, 22301, 27001, 38500 и пр. (например, Cobit в новой версии 5 основан на ISO/IEC, 38500:2008, Corporate Governance of Information Technology). Конечно, в РФ эти стандарты своевременно переводятся в ГОСТ Р ИСО (ИСО/МЭК), но, к сожалению, их правовой статус, определенный в ФЗ-184 «О техническом регулировании», никак не поддерживается ни ФСБ, ни ФСТЭК. Единственный пример — ГОСТ РВ 0015-002 в системе государственного оборонного заказа МО, в котором в п. 4.3 явно указан ГОСТ Р ИСО/МЭК 27001. К сожалению, этого недостаточно для такой страны, как РФ, тем более с учетом известных ограничений и санкций.

Объективно нет оснований полагать, что именно из-за текущей сложившейся ситуации с регулирующими органами все настолько плохо с безопасностью ИТ. Нет, с безопасностью ИТ все совсем неплохо, просто с ней не все достаточно хорошо. Поясним эту мысль подробнее. В России широко и часто безальтернативно используются зарубежные продукты ИТ, которые обладают достаточно адекватной функциональностью в области безопасности (например, операционные системы MS Windows). Надо признать, что функции безопасности продуктов ИТ никак не деградируют при пересечении государственной границы РФ. Ни полупроводниковые компоненты, ни программное обеспечение, ни данные нечувствительны к пересечению границ. Поэтому можно полагать, что с безопасностью все совсем неплохо. А вот доверие к функциональности безопасности продуктов ИТ при пересечении государственной границы очень даже деградирует, особенно по нынешним временам, когда продукты ИТ стали чрезвычайно сложны и поэтому не вполне прозрачны, а правила игры государств, напротив, стали чрезвычайно про-

[3] https://www.securitylab.ru/blog/personal/valerykomarov/343965.php

[4] Членам Ассоциации банков России будет предоставлена возможность подключения к платформе обмена данными о киберугрозах с целью получения самой актуальной информации о злоумышленниках, их методах атак и инструментах. Соответствующие соглашения подписаны 18 июня 2018 г. между Ассоциацией банков России, Bi.zone, техническим провайдером сервиса, а также рядом банков, среди которых «Сбербанк России», Саровбизнесбанк и «Кубань Кредит». На завершающей стадии проработки находится вопрос подключения к платформе еще более 10 банков.
http://safe.cnews.ru/news/line/2018-06-18_rossijskie_banki_obmenyayutsya_dannymi_o_kiberugrozah

[5] В конце 2017 г. Москве состоялось первое заседание клуба «Безопасность информации в промышленности» (БИП-Клуб), объединившего руководителей подразделений информационной безопасности российских предприятий индустриального сектора экономики. Инициатором создания клуба выступил «Норникель». В работе клуба приняли участие представители таких компаний, как «Северсталь», «Энел Россия», НЛМК, «Уралвагонзавод», «Полюс Золото», «ЛУКОЙЛ» и др.
http://norilskiy-nikel.dk.ru/news/237092145

сты и сводятся к беззастенчивой демонстрации силы. Этот аспект может быть рассмотрен на примере системы оценки доверия, точнее фундаментальных различий в двух существующих системах доверия: за рубежом и в РФ. За рубежом принята система оценки доверия на базе «Общих критериев», которая охватывает широчайший диапазон устройств от микросхем до промышленных контроллеров со встроенным программным обеспечением. В РФ действуют национальные системы оценки (сертификации), разработанные ФСТЭК, ФСБ, МО и рядом иных ведомств. К сожалению, применение «Общих критериев» в РФ крайне ограничено даже в таком международном формате, как переводной ГОСТ Р ИСО/МЭК серии 15408. Именно поэтому оценить доверие к функциональной безопасности в РФ весьма проблематично, и приходиться констатировать, что с безопасностью не все достаточно хорошо [6].

Что можно сделать для обеспечения необходимого уровня доверия к функциональности безопасности продуктов ИТ? Кажется, способ решения проблемы очевиден — надо производить продукты ИТ в собственной юрисдикции. Да, это могло бы решить наши проблемы с доверием к безопасности. Но в условиях неадекватности наших регулирующих органов это невозможно. Рассмотрим простой пример. Если вы производите адекватный продукт ИТ с необходимыми заказчикам функциями безопасности без лицензии регулирующих органов, то в итоге вы с высокой вероятностью будете иметь проблемы и после чего уже ничего производить не будете. Если же вы получили все нужные лицензии регулирующих органов, то вы принимаете все их неадекватные требования и переходите к правому пределу, в котором производите неадекватный продукт для защиты информации и имеете проблемы со сбытом, как и многие другие лицензиаты. Поэтому при текущем подходе к безопасности ИТ создание в России адекватных продуктов ИТ с необходимым набором функций безопасности возможно только в режиме «вопреки всему, несмотря ни на что».

Простой и очевидный, принятый в мире подход к созданию продуктов ИТ с функциональностью безопасности –пытаться разработать продукт могут все и без всяких предварительных условий, но сертификацию по требованиям безопасности пройдет только лучший — в России не в почете.

Лирическое окончание

И напоследок в качестве аллегорического представления состояния дел в области ИТ за рубежом и в России приведем два отрывка их стихотворений.

Кейс 1. «ИТ за рубежом»
В. Высоцкий
Чтоб не было следов, повсюду подмели...
Ругайте же меня, позорьте и трезвоньте:
Мой финиш – горизонт, а лента – край Земли, –
Я должен первым быть на горизонте!

Кейс 2. «ИТ в России»
Б. Гребенщиков и группа «Аквариум»
Слишком рано для цирка,
Слишком поздно для начала похода к святой земле.
Мы движемся медленно, словно бы плавился воск;
В этом нет больше смысла -
Здравствуйте, дети бесцветных дней!
Если бы я был малиново-алой птицей,
Я взял бы тебя домой;
Если бы я был...

Как говорится, почувствуйте разницу.

Список литературы

1. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
2. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», далее по тексту упоминается как 15408 часть 1.
3. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», далее по тексту упоминается как 15408 часть 2.
4. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» (Далее по тексту упоминается как 15408. Ч. 3).
5. *Пригожин И., Гленсдорф П.* Термодинамическая теория структуры, устойчивости и флуктуаций. М.: Мир. 1973. 124 с.
6. Надежность и эффективность в технике: Справочник в 10 т. Ред. совет: В.С. Авдуевский, (пред.) и др. М.: Машиностроение, 1988. (в пер.) Т. 3. Эффективность технических систем / Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. 328 ст.: ил.
7. *Лившиц И.И., Неклюдов А.В.* Риски токсичных активов в информационных технологиях // Стандарты и качество. 2017. № 5. С. 20-25.
8. *Лившиц И.И., Неклюдов А.В.* Обеспечение цифрового суверенитета России // Стандарты и качество. 2017. № 8. С. 58-61.

Лившиц Илья Иосифович *– канд. техн. наук, старший научный сотрудник СПИИРАН,*
Неклюдов Андрей Валерьевич *– канд. техн. наук, независимый эксперт.*
Контактный телефон +7 (921) 934-48-46.
E-mail: Livshitz.il@yandex.ru nav7ad@mail.ru