КИБЕРБЕЗОПАСНОСТЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК БИФУРКАЦИЯ НОМЕНКЛАТУРЫ НАУЧНЫХ СПЕЦИАЛЬНОСТЕЙ

Марков А.С.[1]

Уважаемые читатели! Поздравляем всех с Наступившим 2022 годом!

Как принято, мы вступаем в Новый 2022 год с новыми, зачастую весьма смелыми идеями по обеспечению кибербезопасности ресурсов нашей страны. В этом году на то есть свои особые причины. Например, мировые финансовые потери от киберпреступлений в наступившем году ожидаются в 9 трлн долларов, что превышает ущерб от пандемии за два года! Тема кибербезопасности в прошедшем году была отмечена как приоритетная при встрече президентов России и США. В рамках проведения ВЭФ кибербезопасность опять соотнесена с основными рисками человечества и прорывными технологиями IV промышленной революции. Традиционно, в конце уходящего года множество ключевых игроков рынка подготовили аналитические отчеты и обновили топы угроз и рисков. Это не только подтверждает исключительную актуальность тематики, но и позволяет наметить точечные цели и приоритеты в научных исследованиях.

DOI: 10.21681/2311-3456-2022-1-2-9

В России наступивший год принес неожиданный сюрприз в вопросах кибербезопасности, а именно: Минобрнауки России[2] обозначило две (на первый взгляд, идентичные) научные специальности, задающие аналогичный генеральный вектор на поисковые изыскания и защиты диссертаций, а именно:

- 1.2.4 — Кибербезопасность (область: естественные науки, отрасль: физико-математические науки),
- 2.3.6 — Методы и системы защиты информации, информационная безопасность (область: технические науки, отрасль: технические науки).

Надо понимать, что обе специальности возникли не в вакууме — за ними, безусловно, стоят определенные ученые активисты, так сказать, ученые локомотивы и ледоколы российской современной науки, возможно конкурирующие между собой или нет. Как известно, рассматриваемая тематическая область подлежит обязательному регулированию со стороны государства и подразумевает теоретическую проработку научными институтами соответствующих трех служб. Заявлялось, что паспорта специальностей обсуждались в рамках научных мероприятий; думается, задействованы кафедры по информационной безопасности профильных вузов и научно-технические советы организаций, объединяющих суперпрофессионалов по кибербезопасности. Возможно даже был организован мозговой штурм.

Наш журнал, исходя из названия «Вопросы кибербезопасности», максимально заинтересован в корректности и развитии тематического направления, что в итоге сподвигло нас на проведение краткого сравнительного обзора указанных научных специальностей.

Несмотря на то, что специальность по кибербезопасности заявлена в области естественных наук и, по идее, претендует на фундаментальность, — она, на наш взгляд, не может быть изолирована сама в себе и должна «*закономерно открывать новые возможности и методы решения практических задач*». Исходя из этого, сравнительный обзор специальностей имеет смысл проводить не вообще (как «чистой науки»), а в прагматическом смысле – каким именно мировым тенденциям они соответствуют, где полезны и востребованы соответствующие тематические изыскания.

Исходя из этого, представим на суд читателей следующие моменты:

- фиксация понятийного аппарата, соответствующего названиям специальностей;
- краткое сравнение паспортов специальностей;
- краткое представление последних нормативных и профессиональных стандартов как отражение современных инноваций.

2 Портал ВАК при Минобрнауки России. URL: https://vak.minobrnauki.gov.ru/news, ключевые слова: «Проекты паспортов».

1 Марков Алексей Сергеевич, доктор технических наук, CEH, CISSP, главный редактор журнала «Вопросы кибербезопасности». Москва, Россия. E-mail: editor@cyberrus.com

Рис. 1. Основные факторы свойств системы

Приоритизацию подпунктов паспортов мы опускаем, исходя из традиционной «стабильности» современных институтов науки и чрезвычайной динамичности тематики: картина топов угроз и атак через год кардинально поменяется, а паспорта – нет.

Понятийный аппарат кибербезопасности и информационной безопасности

Дефиниция «информационная безопасность» (ИБ) у нас в стране сложилась и опирается на международные стандарты европейского происхождения. Согласно ГОСТ Р ИСО/МЭК 27000, **информационная безопасность характеризует сохранение свойств конфиденциальности, целостности и доступности информации (КЦД)**[3]. В литературе встречаются творческие, в том числе нестрогие определения, например, некоторые авторы декларируют ИБ не как свойство (состояние), а как процесс. Будем считать, что процесс целесообразно сформулировать как «обеспечение ИБ» (в самом узком варианте – «защита данных»).

Согласно теории систем, основополагающим фактором ИБ является именно **угроза** в информационной сфере (рис. 1). Отсутствие угрозы конкретному информационному ресурсу (активу) обуславливает отсутствие предмета обсуждения.

Напомним, что в зависимости от этапов жизненного цикла изделия в защищенном исполнении рассматривают кортеж базовых факторов: **дефект безопасности** (weakness), **уязвимость** (vulnerability), **угроза, риск**. Именно адекватность и полнота систематик и таксономий указанных факторов обуславливают уместность, результативность и эффективность методов обеспечения ИБ.

Что касается второго понятия — «**кибербезопасность**», то в отличие от ИБ оно имеет американское происхождение. И зачастую носит нестрогий (dumbed-down [1, с. 11]) характер по причине популяризации в СМИ или же отождествления с военными операциями в киберпространстве как новом театре военных действий, как-то: кибероперация «Олимпийские игры» (Stuxnet) [2]. В стандартах указанный американизм представлен условно двумя трактовками:

- как выраженная активная составляющая (offensive security) ИБ, а именно — **свойства защищённости компьютерных ресурсов от компьютерных** (обычно целенаправленных) **атак**[4];
- **как синоним** ИБ в некотором сегменте компьютерного пространства (фактически, это сленг ИБ), то есть — как свойства защищенности сегмента компьютерных ресурсов (или данных в электронном виде, или абстрактных виртуальных приложений) от соответствующих компьютерных угроз в традиционной парадигме КЦД[3].

Первый, «пронаступательный» вариант дефиниции приводится в глоссариях Комитета по системам национальной безопасности США (CNSSI) и Национального института стандартов и технологий США (NIST), а также в ряде американских нормативно-методических фреймворках и пр. [3]. Разумеется, аналогичной позиции придерживаются практикующие ученые по кибербезопасности НАТО[5]. Ряд специальных публикаций NIST вообще дефиницию сводит тривиально к «*предотвращению, обнаружению и реагированию на атаки*»[6]! Очень важно, что здесь эффективность методов кибербезопасности напрямую зависит от таксономии компьютерных атак. Виды, категории, этапы («техники»), методики («тактики») и средства проведения компьютерных атак и составляют **суть тематики кибербезопасности** как ее трактует первоисточник.

Второй, «сленговый» вариант тоже весьма распространен, его модификации приводятся в американских политических документах[7], словарях и т.д. [4].

Можно повторить, что в литературе (например, [5-11]), интернет-блогах и постах можно встретить некоторые производные указанных определений, но в целом отмечаются именно две отличительные черты понятия кибербезопасности:

- наличие угрозы реализации компьютерной атаки (как активной наступающей сетевой составляющей свойства ИБ) и/или
- цифровые ресурсы, подлежащие компрометации.

3 По ГОСТ, кроме КЦД, могут быть добавлены свойства подлинности, подотчетности, неотказуемости, надежности, по ISO — еще свойство доверия (trustworthiness), по Паркеру — еще свойства контролируемости владельцем (possession) и полезности.

4 (Англ.) Cybersecurity — the ability to protect or defend the use of cyberspace from cyber attacks [NISTIR 8170:2021, CNSSI 4009:2015].

5 NATO CCDCOE, URL: https://ccdcoe.org/library/publications/

6 NIST SP 800-160, NISTIR 8183, NISTIR 8183A.

7 (Англ.) Cybersecurity — prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [US Presidential Directive NSPD-54/HSPD-23).

DOI:10.21681/2311-3456-2022-1-2-9

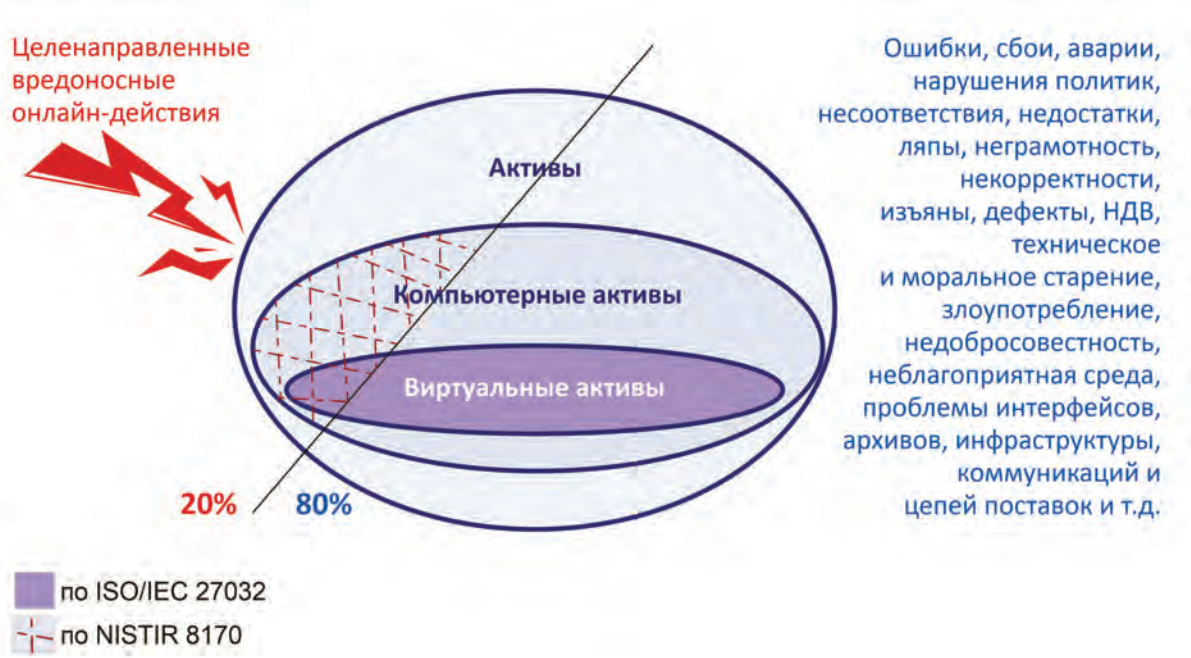

Рис. 2. Сфера кибербезопасности по ISO/IEC 27032 и NISTIR 8170

Что касается географии остального научно-технического мира, то понятие кибербезопасности остается дискуссионным, хотя термин уже упоминается (вне общего глоссария) во всех трех системах международной стандартизации ISO, IEC и ITU. Так, стандарт ISO/IEC 27032:2012 трактует кибербезопасность по аналогии с американским сленговым понятием, категорически его сужая виртуальной средой, не имеющей вещественной формы (как-то: QR-код, криптовалюта, транзакция, но никак не USB-флешка или Wi-Fi-роутер). Новый стандарт ISO/IEC 27100:2020 дает определение кибербезопасности как свойства защищенности активов (общества, организации, человека) от киберрисков, связанных с **эксплуатацией уязвимостей** в киберпространстве – цифровой среде в самом широком смысле. Подобную интерпретацию дает технический стандарт ITU X.1205: 2008: те же угрозы и риски КЦД[3] в ограниченной (сетевой) среде. Упоминание рисков, по мнению авторов нормативных документов, подчеркивает проактивную деятельность по управлению кибербезопасностью. Демонстрация определений представлена на рис. 2.

Можно добавить, что американизм прижился не везде. Например, Совет Безопасности Российской Федерации и МИД России аргументировано предпочитают вместо термина «кибербезопасность» использовать формулировку «безопасность в ИКТ-среде» [12].

В табл. 1 приведены ключевые аспекты кибербезопасности и информационной безопасности.

Таким образом совершенно очевидно, что мировое сообщество рассматривает кибербезопасность **CS** как часть и только часть ИБ — **IS**:

$$\mathbf{IS} \subset \mathbf{CS}_i, \qquad (1)$$

где i – индекс итерации парадигмы проблематики безопасности.

Легко увидеть, что методы ИБ и кибербезопасности имеют ярко выраженные прикладные цели, задачи и реализации, то есть лежат, главным образом, в плоскости технических наук, но, разумеется, – как любая сложная проблематика – на стыках и пересечениях, например, военных, социальных, юридических, политических и др.

Метаморфозы паспортов специальностей кибербезопасности и информационной безопасности

Итак, если посмотреть на паспорта специальностей 1.2.4 и 2.3.6, становится совершенно очевидно, что для их формирования использовался не столько системный подход (актуальные классы угроз и рисков относительно всего спектра механизмов безопасности и приложений), сколько наработки уважаемых научных школ.

Дайджесты из паспортов специальностей[8,9] (полный текст можно посмотреть на обложке журнала) представлены на рис. 3.

Не представляет труда увидеть, что в отдельных случаях имеет место быть пересечения (мы условно их на рис. 3 отметили одинаковыми цветами). Это и ожидаемо, исходя из определения понятийного аппа-

8 Паспорт 1.2.4. URL: https://drive.google.com/file/d/1As4dPAHxCrquvI9-wxEMw2Oto2sgMjr1/view

9 Паспорт 2.3.6. URL: https://drive.google.com/file/d/1ofuvg97Nw0smDpSA_VNphXKFrF-Ngjq-/view

Таблица 1

Ключевые аспекты понятий кибербезопасности и информационной безопасности

ФОКУС	Кибербезопасность	Информационная безопасность
Таксономии	ATT@CK, Cyber Kill Chain	SCAP (CWE, CVE, ...) и др.
Киберкоманды	Cyber red teams (CRT)	Все цвета
Сертификаты	CEH, OSCP	CISSP, CISA, CISM
Факторы безопасности	Уязвимости	Дефекты безопасности, уязвимости, угрозы, риски
Угрозы	Возможность проведения компьютерной (целенаправленной) атаки на компьютерные ресурсы	Все виды угроз, в том числе непреднамеренные, в том числе всем ресурсам, угрозы среды и цепочек поставки
Нарушения (реализация угрозы)	НСД (путем эксплуатации уязвимости или выполнения парольной атаки) или отказ в обслуживании	Нарушение целостности, доступности, конфиденциальности и др.
Источники воздействия	Хакеры и кибергруппировки (противник)	Все внутренние и внешние субъекты и активные объекты, среда безопасности, инфраструктура и пр.
Процессы	Разведка, атака, скрытие следов	СМИБ, включая политики (роли и обязанности), BC/DR-планы, риск-менеджмент, организационно-технические меры (детективные, превентивные, восстановительные, директивные и др.), механизмы безопасности (IA4, IDS/IPS, DLP, VA, AV, FW, SIEM и др.), SDL, сертификация, аттестация, спецэкспертизы, СИ/СО/СП и пр.
Данные	Конкретные технические данные (хеши, пароли, ключи, адресные данные) и наборы данных (фрагменты трафика, логи и пр.)	Все виды данных, всех форматов и форм, в том числе электронные, в твердой копии, программный код, документация, файловые системы, БД, архивы, хранилища, облака, big/smart data и пр.

рата. При этом наиболее дискуссионным становится даже не вопрос дублирования, а вопрос каким образом кибербезопасность как прикладная техническая область попала в раздел естественных наук (1.2.4). Можно предположить, что истоки стоят в теоретических изысканиях проектирования моделей доверенных (или наоборот, 0-доверенных, как сейчас модно говорить) программ как направления теоретической информатики. При этом мы сознательно опускаем пятидесятилетнюю научную дискуссию о результативности и эффективности изысканий по верификации и формализации программ и спецификаций. Думается, факт отнесения кибербезопасности к фундаментальным изысканиям озадачит любого специалиста по кибербезопасности (этичного хакера), по крайней мере, сейчас.

Что касается паспорта специальности по информационной безопасности (2.3.6, пока 05.13.19), то отрадно, что в новый паспорт вошла, наконец, тематика приложений криптографии, однако, надо понимать, что она лежит на стыке физико-математических и технических наук (что из текущей версии паспорта специальности не видно).

Возможно, авторы паспортов постарались развести модный мейнстрим по разным научным областям и отраслям. В ироничном смысле мы столкнулись с котом Шредингера (в данном случае, киберкотом) — когда кибербезопасность одновременно является и частью ИБ (то есть имеет совершенно конкретный прикладной научно-технический смысл и которая зиждется на теоретическом базисе и аппарате множества точных наук и их производных, а также экспериментах), и наоборот – кибербезопасность стала предметом области естественных наук (а-ля «зловредология», причем метафизическая, так как заявлены защиты диссертаций исключительно по отрасли физ.-мат. наук), которая в буквальном смысле должна бы стать неким фундаментальным базисом «Матрицы» будущего.

Можно добавить, что омонимы в науке имеют место быть (электрический градус и градус Гесса), но проблема в том, что содержание паспортов не позволяет сделать вывод о подмене понятий – они конгруэнтны. И усиление положений фразами, типа ИИ или «глубокий» — не имеет никакого значения и применимо для многих научных специальностей.

DOI:10.21681/2311-3456-2022-1-2-9

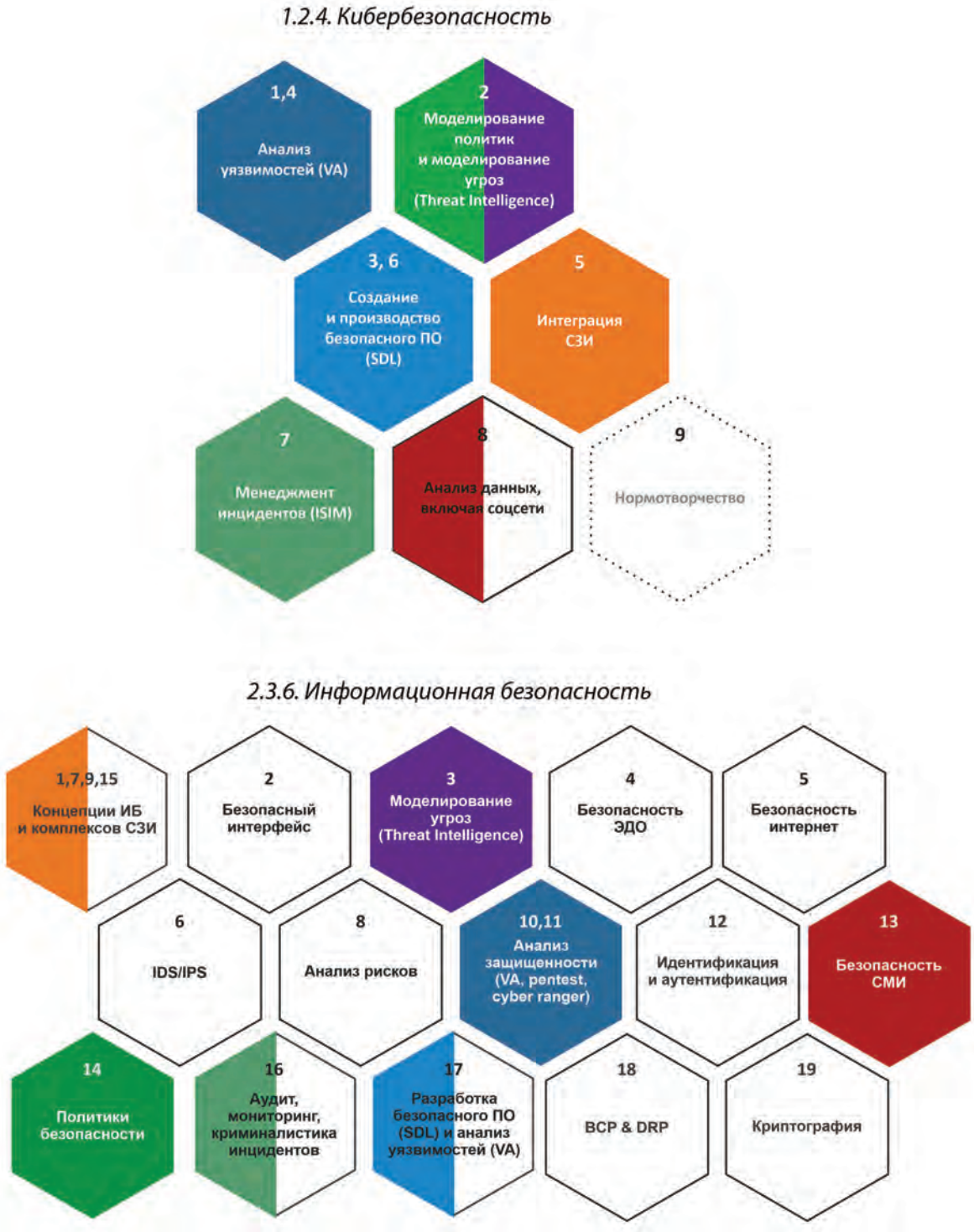

Рис. 3. Сравнение паспортов специальностей 1.2.4 и 2.3.6

Образовательный стандарт как зеркало востребованности тематики кибербезопасности

Отдельно хотелось бы затронуть вопрос, как видят кибербезопасность профессиональные образовательные сообщества. Требования к обучению в индустриальных странах формируются не просто так – они являются обязательной ступенью при занятии определенной должности на госслужбе. Косвенным признаком востребованности соответствующих сертифицированных специалистов является заработная плата на сайтах вакансий. Наиболее авторитетными системами сертификации специалистов по ИБ являются Междуна-

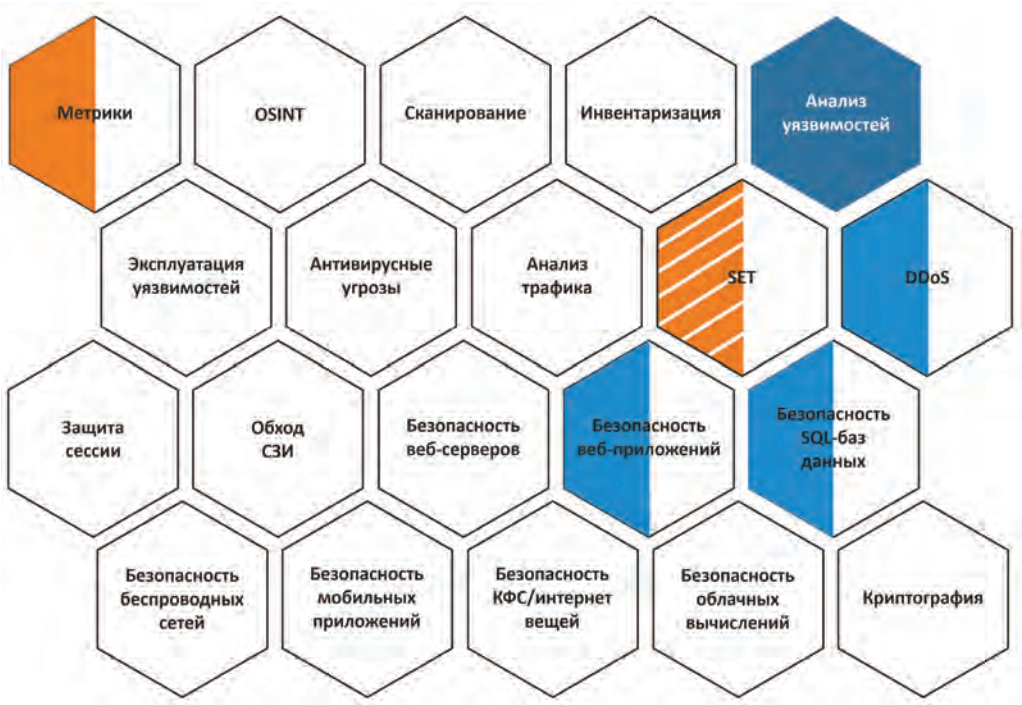

Рис. 4. Востребованность тематик кибербезопасности согласно EC-Council

родный консорциум по сертификации безопасности информационных систем — (ISC)2, Ассоциация аудита и контроля информационных систем – ISACA, Ассоциация индустрии вычислительных технологий – CompTIA, а по кибербезопасности — Международный совет консультантов по электронной торговле – EC-Council и международная компания Offensive Security LLC[10]. Посмотрев соответствующие требования по подготовке специалистов, можно сформировать взгляд на востребованность тематик в проекции на **перспективные исследования** в интересах страны.

Так, ниже на рис. 4 приведены домены по подготовке специалистов по кибербезопасности по версии EC-Council. Мы немного домены подкрасили, где предположили гипотетическую связь с пунктами паспорта 1.2.4. Легко заметить, какой имеется разрыв между пониманием сути кибербезопасности со стороны новой номенклатуры и международными профильными стандартами.

Комплекс мер кибербезопасности как один из признаков полноты

Ниже в табл. 2 приведены контрмеры по кибербезопасности согласно «Рекомендациям по кибербезопасности» ISO/IEC 27032. Однако сравнить его с паспортом специальности 1.2.4 весьма затруднительно по очевидным причинам – оставим этот ребус любознательному читателю. Думаем, картина будет еще печальнее, чем показанная выше.

Заключение

В настоящее время российская наука, несомненно, переживает волнующий виток своего прогрессивного развития в виде введения новых и обновленных паспортов научных специальностей[11]. По общему мнению – «шаг вперед»[12].

Одним из феноменов указанного процесса является появление схожих на первый взгляд паспортов специальностей в сфере информационной безопасности, но разведенных по разным областям науки: естественным и техническим. Разумеется, это повлечет распараллеливание научных структур [13], порождение дилеммы выбора, рост «проклятой» неопределённости, конформизм. Является ли это знаком добавления новой степени свободы научного творчества или же наоборот, под угрозой строгость научных положений, — «шаг вперед» или «шаг вперед, два шага назад» – покажет время.

А пока с этим придется просто жить, разделив обеспечение кибербезопасности строго на технические эксперименты и абстрактные умозаключения.

Если сравнить оба паспорта специальностей (1.2.4 и 2.3.6), то мы видим не только пересечения (налицо противоречивость номенклатуры научных специальностей), но и вопрос об их полноте. Очевидно, что в этом плане паспорт 2.3.6 выигрывает (см. рис. 3). Это связано с тем, что многие практикующие ученые в мире ИБ, принявшие участие в обсуждении новой но-

10 https://hackr.io/blog/best-cybersecurity-certification

11 https://regulation.gov.ru/projects#npa=111185

12 https://www.pnp.ru/social/v-rossii-poyavyatsya-doktora-nauk-po-kiberbezopasnosti.html

Таблица 2

Организационно-технические меры по кибербезопасности

Категория безопасности	Мера безопасности
Безопасность приложений	Уведомление пользователей о политике безопасности
	Защита сессий веб-приложений
	Контроль корректности вводимых данных (защита от SQL-инжекций)
	Обеспечение безопасности скриптов (защита от атак межсайтового скриптинга)
	Аудит кода и независимое тестирование программного кода
	Подтверждение подлинности провайдера для потребителей
Безопасность серверов	Безопасное конфигурирование серверов
	Установка системы обновлений безопасности
	Контроль системных журналов
	Защита от вредоносных программ
	Регулярное сканирование контента на наличие вредоносных программ
	Регулярное сканирование уязвимостей сайта и приложений
	Обнаружение попыток взлома
Безопасность конечных пользователей	Использование рекомендованных версий операционных систем
	Использование рекомендованных версий программных приложений
	Использование антивирусных средств
	Настройка веб-браузеров в безопасном режиме
	Блокировка или безопасное выполнение скриптов
	Использование фильтров фишинга
	Использование дополнительных механизмов безопасности веб-браузеров
	Использование персональных межсетевых экранов и систем обнаружения вторжений
	Использование автоматических обновлений доверенных программ
Защита от атак методами социальной инженерии	Разработка и внедрение политик безопасности
	Категорирование и классификация информации
	Обучение и повышение осведомленности пользователей
	Тестирование сотрудников
	Мотивация и стимулирование сотрудников
	Использование технических механизмов контроля
Повышение готовности	Использование ловушек в «пустой» сети
	Перенаправление вредоносного трафика
	Обратная трассировка

менклатуры, имеют конкретные внедрения научных результатов (как это принято именно в технических науках) и подтвердили их значимость путем апробации, например, по требованиям приказов ФСТЭК России, международных стандартов 27000-серии или стандартов Банка России, которые блестяще систематизированы. Что касается собственно тематики кибербезопасности, то она остается «инновационной», так как ее терминология в России пока не состоялась и в противоположность всем общемировым тенденциям, и даже к стандарту ISO/IEC 27032:2012 в профильных отечественных технических комитетах относятся с предельной осторожностью. Возможно, многие ученые светила и рыцари науки опустили руки после оглушительного краха создания национальной стратегии по кибербезопасности в 2014 году [14].

Уверены, что отмеченные «отдельные некорректности» новой номенклатуры паспортов со временем будут нивелированы с учетом риск-ориентированного подхода.

Редакция приглашает всех увлеченных тематикой ученых к конструктивной позитивной дискуссии и к публикации новых результатов авторских исследований по всей проблематике информационной безопасности на страницах нашего журнала в наступившем Новом 2022 году и далее!

Главный редактор
Certified Ethical Hacker (EC-Council),
Certified Information Systems Security Professional (ISC)2,
доктор технических наук

Алексей Марков

Литература

1. Brookson C. and etc. Definition of Cybersecurity. Gaps and overlaps in standardization. ENISA, 2015, TP-01-15-934-EN-N, 32 p. DOI: 10.2824/4069.
2. Харрис Ш. Кибер войн@. Пятый театр военных действий — М.: Альпина нон-фикшн, 2016. — 390 с.
3. Möller D.P.F. Cybersecurity in Digital Transformation. Scope and Applications. Springer, 2020. 126 p. DOI: 10.1007/978-3-030-60570-4.
4. Wilson D.C. Cybersecurity. MIT, 2021, 160 p.
5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 4 (38). С. 39-42.
6. Архипова Е.А. Современное понимание терминов «кибернетическая безопасность» и «информационная безопасность» // Young Scientist, 2019, № 12(76), pp. 315-320. DOI:10.32839/2304-5809/2019-12-76-67.
7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность — подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22-27.
8. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С. 2-9.
9. Кузьмин А., Жуков Ю., Финогенов Д. Терминология в сфере международной информационной безопасности // BIS Journal, 2015, №3 (18).
10. Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity // Technology Innovation Management Review. 2014, No 10, pp. 13-21.
11. Starodubtsev Y.I., Balenko E. G., Vershennik E.V. and Fedorov V. H. Cyberspace: Terminology, Properties, Problems of Operation. In: International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 2020, pp. 1-3, DOI: 10.1109/FarEastCon50210.2020.9271282.
12. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. — М.: МГИМО, 2021. — Том 1 (2-е изд., доп.) — 384 с.
13. Фрадков А. Кибернетика опять лженаука? // Троицкий вариант — Наука. 01.12.2020 — № 318 — с. 4.
14. Гаттаров Р.У. Концепция стратегии кибербезопасности // Вопросы кибербезопасности. 2014. № 1(2). С. 2-4.

Паспорта научных специальностей

1.2.4. Кибербезопасность

Область науки: 1. Естественные науки.
Группа научных специальностей: 1.2. Компьютерные науки и информатика.
Наименование отрасли науки, по которой присуждаются ученые степени: физико-математические науки.

Направления исследований:
1. Анализ известных и вновь выявляемых уязвимостей, их систематизация, разработка методов интеллектуального поиска новых классов уязвимостей.
2. Моделирование политик информационной безопасности, угроз и атак, методические основы разработки профилей защиты.
3. Методы проектирования, моделирования, анализа, трансформации программ для выявления потенциальных уязвимостей в программных системах с учетом специфики фаз жизненного цикла: разработки требований, проектирования архитектуры, разработки программного кода, тестирования, верификации, сертификации и эксплуатации.
4. Методы, алгоритмы и средства пострелизного глубокого анализа защищенности программно-аппаратного обеспечения.
5. Методы интеграции средств защиты на уровне аппаратуры и на уровне программного обеспечения.
6. Методы, алгоритмы и средства обеспечения устойчивого функционирования программно-аппаратных систем в условиях злонамеренного воздействия включая методы обфускации и безопасной компиляции программ.
7. Интеллектуальный масштабируемый мониторинг инцидентов безопасности в распределенных программно-аппаратных системах, методы оперативного реагирования на выявленные угрозы.
8. Масштабируемые средства интеллектуального анализа данных и процессов в распределенных системах, включая социальные сети.
9. Разработка методических основ для создания и развития метрик оценки защищенности, уровня доверия компьютерных систем и стандартов в области кибербезопасности.

2.3.6. Методы и системы защиты информации, информационная безопасность

Область науки: 2. Технические науки.
Группа научных специальностей: 2.3. Информационные технологии и телекоммуникации.
Наименование отрасли науки, по которой присуждаются ученые степени: технические науки.

Направления исследований:
1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.
5. Методы, модели и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
7. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
10. Модели и методы оценки защищенности информации и информационной безопасности объекта.
11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
13. Исследования и разработка методов в области выявления и противодействия распространению ложной и вредоносной информации.
14. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
16. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
17. Методы, модели и средства разработки безопасных программ, выявления дефектов безопасности в программном обеспечении, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.
18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.
19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.