О НОВОЙ НОМЕНКЛАТУРЕ НАУЧНЫХ СПЕЦИАЛЬНОСТЕЙ И НЕ ТОЛЬКО…

Минзов А.С.[1]

Уважаемые читатели!

Введение новой Номенклатуры научных специальностей всколыхнуло научную среду и в основном получило положительную оценку. Однако, как и в любом важном начинании, не обошлось без досадных огрехов. В частности, это коснулось научных специальностей в области кибербезопасности. Если сравнить ученые степени ученых, работающих в этой области, то подавляющее их число имеют степени докторов и кандидатов технических наук, а меньшее число – докторов и кандидатов физико-математических наук, что вполне естественно, так как последние работают в ограниченном сегменте кибербезопасности: криптографии и стеганографии.

Редакция предлагает очередное мнение по этой проблеме.

Проблемы введения новой научной специальности «1.2.4.Кибербезопасность» в области естественных наук

К сожалению, сегодня термин «кибербезопасность» не имеет четкого содержания. Рассмотренные определения этого термина в работах [2-4] имеют настолько противоречивые трактования, что невозможно четко определить область научного исследования по этой специальности. Это означает, что и паспорт специальности кибербезопасности будет также таким же: нечётким, размытым и неопределенным. При этом остается главный вопрос, нужна ли необходимость выделения научной специальности «***1.2.4.Кибербезопасность***» в отдельное научное направление, если уже есть и достаточно долго используется другая специальность «***2.3.6.Методы и системы защиты информации, информационная безопасность***» ? Ответ на этот вопрос достаточно очевиден, если определить четкие границы разделения этих научных специальностей и выделить проблемы, решаемые этими специальностями. К сожалению, такого обоснования сегодня нет, а приведенные в статье А.С. Маркова [2] аргументы свидетельствуют о значительном совмещении задач, решаемых в этих научных специальностях, вплоть до совпадения определений «***информационная безопасность***» и «***кибербезопасность***» как конфиденциальность, целостность и доступность информации. Однако, это далеко не так и мы попробуем привести аргументы о необходимости и условиях такого разделения на современном этапе развития теории и методологии создания систем защиты информации.

Прежде всего, следует отметить, что понятие «***кибербезопасность***» уже практически вошло в нашу жизнь и это подтверждают соответствующие отечественные и международные стандарты, относящиеся к киберфизическим системам, интернету вещей и кибербезопасности. Понятие «***киберпространство***» также не имеет сегодня четкого определения и, с точки зрения технических решений по организации защиты информации, может трактоваться как *сложная среда, включающая в себя информационные и автоматизированные системы управления, построенные на основе глобальных информационных и коммуникационных технологий*[2]*. Это дает большие технические преимущества при решении сложных задач в информационных и автоматизированных системах управления, но одновременно создает и дополнительные угрозы для этих систем. Поэтому возникает необхо-*

2 Это определение автора, что не исключает и другие формулировки, например при создании философских концепций обмена информацией в киберпространстве.

1 Минзов Анатолий Степанович, доктор технических наук, профессор кафедры безопасности информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail:minzav@mpei.ru

*димость научно-методического развития методов и технологий защиты информации в киберпространстве. На наш взгляд, содержания терминов «кибербезопасность», «киберпространство» и «киберугроза» непосредственно связано с термином «**кибернетика**»*, который определяется как наука об управлении [5] и в терминологии новой номенклатуры специальностей трактуется как «***1.2.3.Теоретическая информатика. Кибернетика***». Отсюда вполне естественно возникает и научное направление «***1.2.4.Кибербезопасность***», связанное с разработкой научной теории применения принципов, методов, математических моделей, алгоритмов и технологий обеспечения безопасности систем управления в киберпространстве. Это позволяет нам рассматривать кибербезопасность как систему защиты информационных и автоматизированных систем управления в киберпространстве от киберугроз и кибератак, позволяющую обеспечить:

1) ***непрерывность её функционирования*** (способность системы управления восстанавливать параметры своего состояния при прерываниях и остановках процессов в допустимые сроки);
2) ***эффективность системы управления*** в соответствии с заданными конечными целями управления системой [6];
3) ***устойчивость сохранения параметров*** системы управления (свойство гомеостаза системы [7], позволяющее сохранять допустимые параметры функционирования систем управления при определенных изменениях параметров киберпространства);
4) ***надежность*** (свойство системы управления сохранять в определенном времени способность выполнять требуемые функции в заданных режимах и условиях применения) [8];
5) ***требуемый уровень доверия*** к системе кибербезопасности [9];
6) ***возможность адаптации системы управления*** к новым и нештатным ситуациям.
7) **обоснование структуры системы кибербезопасности на основе цифровой модели управления рисками** [10,11].

Такая постановка задачи кибербезопасности, как нового научного направления, позволяет выйти на принципиально новый уровень создания информационных и автоматизированных систем управления в киберпространстве. Сегодня в такой постановке эти задачи рассматриваются весьма ограниченно при автоматизированном проектировании АСУ с использованием SCADA-систем и, как правило, вне связи с направлением кибербезопасности. Предлагаемый подход позволяет решать задачи, о которых мы сегодня еще не говорим, но они появятся в ближайшем будущем, например:

— создание защищенных информационных систем, способных к реконфигурации при кибератаках в условиях сохранения приоритетных функций в системе управления;
— создание цифровых моделей систем кибербезопасности (цифровых двойников) для обоснования принимаемых решений в различных ситуациях;
— создание систем с заданными критериями эффективности и обеспечивающими гарантированные параметры безопасности для критических информационных инфраструктур в киберпространстве[3] и другие задачи.

Мы не будем раскрывать детально эти требования к системе кибербезопасности, во многом они очевидны и требуют дальнейшего обсуждения при разработке паспорта этой специальности. Следует отметить, что задачи, решаемые кибербезопасностью, значительно шире, чем определенные требованиями существующих нормативных документов по информационной безопасности, в том числе и для КИИ, и нацелены на конечные результаты работы систем управления в киберпространстве.

Заключение

Появление новой научной специальности «***кибербезопасность***» имеет смысл только в том случае, если в ней рассматриваются вопросы, касающиеся информационной безопасности систем управления в сложной информационно-коммуникационной среде киберпространства при воздействии на них кибератак. Следовательно, цели защиты информации будут непосредственно связаны с целями функционирования систем управления. Такая концепция сегодня существует и реализована во фреймворках COBIT 5.0 и COBIT 2019 [12,13]. По существу, в этих концепциях информационная безопасность рассматривается, как обеспечивающая функция и реализуется в значительной степени при проектировании информационной технологии.

1. Хочу остановиться ещё на одном аспекте, связанным с научной специальностью «***кибербезопасность***». Это касается отрасли науки, по которой присваивается учёная степень: физико-математические науки. На наш взгляд, это научное направление связано в большей степени с архитектурным и концептуальным проектированием системы кибербезопас-

3 Сегодня практически все объекты энергетики по генерации, трансферу и распределению электроэнергии относятся к системам киберпространства.

ности на основе управления рисками. При этом используются как точно заданные параметры системы, так и измеряемые в форме лингвистических переменных, что вызывает необходимость применения механизмов нечетких множеств, логики и величин для получения более устойчивых к ошибкам оценок вычисляемых параметров (возможностей реализации угроз, уязвимостей и оценок рисков). Кроме того, для классификаций киберугроз будут использоваться также нейросетевые модели, деревья решений и другие приложения, которые обычно применяются для решения технических научных задач. Поэтому вполне естественно включить в качестве отрасли по этой специальности дополнительно ученую степень *технических наук*. Это расширит возможности диссертационных советов и позволит давать адекватные оценки отраслевой классификации защищаемым диссертациям.

2. Несколько слов о научной специальности «*2.3.6.Методы и системы защиты информации, информационная безопасность*». Безусловно, что это научная специальность должна сохраниться при некоторой модернизации содержания паспорта специальности. На наш взгляд, в паспорте этой специальности должны найти отражение научные проблемы создания эффективных технических решений по различным концепциям защиты информации в информационных системах и АСУ, в том числе [14]:

- Концепции, основанной на процессном подходе и управлении рисками на основе циклов управления PDCA или более современных циклов с дополнительными этапами: обоснования необходимости разработки СМИБ, выявления проблем и возможностей организации для создания СМИБ, разработкой маршрутной карты и оценкой эффективности реализации цикла управления.
- Концепции гарантированной защиты на основе классификации необходимой степени защищенности ИС для обеспечения информационной безопасности информации ограниченного доступа.
- Концепции проактивной защиты на основе киберразведки, анализа событий и прогнозирования сценариев реализации угроз информационной безопасности.
- Концепции, основанные на обеспечении непрерывности бизнес-процессов.
- Концепция восстановления системы безопасности при появлении инцидентов.
- Различные сочетания этих концепций.

Список использованных источников

1. Приказ Министерства науки и высшего образования Российской Федерации от 24.02.2021 № 118 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утвержденное приказом Министерства образования и науки Российской Федерации от 10 ноября 2017 г. № 1093».
2. Марков А.С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. – 2022. – №. 1 (47). – С. 2-9.
3. ISO/IEC 27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
4. Концепция стратегии кибербезопасности Российской Федерации http://www.council.gov.ru/media/fi les/41d4b3dfbdb25cea8a73.pdf
5. Norbert Wiener. Cybernetics or Control and Communication in the Animal and the Machine. (Hermann & Cie Editeurs, Paris, The Technology Press, Cambridge, Mass., John Wiley & Sons Inc., New York, 1948)
6. Энциклопедия кибернетики» под ред. В. М. Глушкова, т.1., Киев, 1974.
7. Горский Ю. М. и др. Гомеостатика живых, технических, социальных и экологических систем. – Новосибирское отделение издательства» Наука», 1990.
8. ГОСТ 27.002-2015 . Межгосударственный стандарт. Надежность в технике. Термины и определения.
9. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
10. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с. : ил.
11. Минзов А.С., Черемисина Е.Н., Токарева Н.А., Бобылева С.В. Моделирование рисков информационной безопасности в цифровой экономике: монография/ Под редакцией А.С. Минзова. — М. : КУРС, 2021. — 112 с. : ил.
12. COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
13. Anne Milkovich, CGEIT ISBN 978-1-60420-237-3. URL: https://www.mitigasibencana.bpbd.kotabogor.go.id/uploads/edukasi/COBIT5.pdf (дата обращения: 28.01.2022).
14. Andrey Prozorov COBIT 2019 для СУИБ. URL: https://www.securitylab.ru/blog/personal/80na20/348063.php (дата обращения: 28.01.2022).
15. Минзов А.С., Баронов О.Р., Минзов С.А., Осипов П.А. Управление событиями информационной безопасности: Учебное пособие / Под редакцией профессора, д-ра техн. наук А.С. Минзова. — М. : ВНИИгеосистем, 2020. — 97 с. : ил.