DOI:

ГАРМОНИЗАЦИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ СИСТЕМ КОРПОРАТИВНОГО И ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ

Михалевич И.Ф.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
mif-orel@mail.ru

Аннотация: Работа посвящена исследованию проблем обеспечения кибербезопасности интегрированных цифровых систем корпоративного и технологического управления, вызванных ускоренной цифровизацией систем технологического управления, их интеграции с цифровыми системами корпоративного управления, «цифровым неравенством» интегрируемых систем в части защищенности от кибератак из открытого информационного пространства

Ключевые слова: информационная безопасность, кибербезопасность, корпоративное управление, критерии безопасности, промышленная автоматизация и управление, технологическое управление, цифровое неравенство, цифровая экономика

Введение

Цифровизация затрагивает сферы жизни, которые ранее могли быть не связаны между собой. По мере цифровизации системы, функционирующие на основе информационных технологий, как правило становятся связанными между собой единой средой Интернета. С Интернетом связано также построение и развитие цифровой экономики, под которой понимается хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг (Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы, утверждена Указом Президента Российской Федерации от 09.05.2017 г. № 203).

Данные в цифровом виде давно существуют в информационных системах и корпоративных системах управления. В меньшей степени цифровизацией были охвачены автоматизированные системы управления, что вызвало процессы под названием «цифровая трансформация» АСУ. Цифровая трансформация вызывает не только замену аналогового оборудования на цифровое, но и массовое подключение АСУ к Интернету, без принятия необходимых мер защиты от угроз, ранее не существовавших в этих изолированных АСУ, развитие систем промышленной автоматизации и управления (СПАУ, IACS - Industrial Automation and Control Systems).

Цифровизация вызвала многие новые проблемы в сфере обеспечения безопасности (термин АСУ ТП устаревает, но применяется в действующих нормативных актах и обзорах по безопасности), что, на взгляд автора, послужило катализатором интеграционных процессов и гармонизации подходов к защите любых систем, основанных на информационных технологиях и Интернет, появлению термина «критическая информационная инфраструктура». Согласно Федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» критическую информационную инфраструктуру (КИИ) образуют информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления и сети электросвязи, используемые для организации взаимодействия названных систем.

Далеко не все системы КИИ одинаково защищены в силу их «цифрового неравенства» [1], что необходимо учитывать в методологии развития КИИ.

1 Трансформация вектора кибератак

Глобальная цифровизация первоначально пошла по пути применения наиболее общих принципов проектирования сетевой инфраструктуры, использования наиболее популярных операционных систем и протоколов передачи данных. Делалось это, как правило, без учета основ построения защищенных систем, провозглашающих принцип комплексирования функциональных требований и требований безопасности, обязательность моделирования угроз безопасности, разработки комплекса мер противостояния угрозам, создания подсистем защиты, текущей оценки угроз и реагирования на них на всех этапах жизненного цикла систем.

Ускоренная цифровизация повлекла множественные нарушения безопасности в результате кибератак, особенно на АСУ ТП. Например [2], проникновение в 2010 году вредоносной программы Stuxnet на объекты ядерной промышленности Ирана, атака на АСУ ТП коммунальной компании Kemuri Water Company в 2015 году (злоумышленники смогли изменить количество химических реагентов, используемых в ходе очистки водопроводной воды), кибернападение на термальную солнечную электростанцию Ivanpah Solar Electric Generating System в 2016 году (привело к возникновению пожара из-за нарушения порядка позиционирования зеркал), атака на металлургическое предприятие Norsk Hydro в 2019 году (вышло из строя 22 000 рабочих мест пользователей на 170 различных объектах в 40 странах. Пострадали как офисные, так и технологические процессы; заражению подверглись промышленные сети, из-за чего часть производства была заблокирована), проникновение программы-шифровальщика в АСУ компании «Одинцовский Водоканал» в 2019 году (под угрозой оказались сохранность технической документации и данные об абонентах компании).

Анализ промышленного интернета вещей (Industrial IoT, IIoT) и производственных систем [3] показал, что целями злоумышленников могут быть как промышленный шпионаж и финансовая выгода, так и попытки саботировать производственный и другие процессы. Точки вхождения: АРМ операторов и инженеров поддержки и разработки, системы управления производством (MES), интерфейсы управления «человек-машина» (HMI), базы данных и внешние подключаемые библиотеки. К основным векторам обнаруженных атак были отнесены:

- компрометация инженерного АРМ через вредоносный add-in или уязвимости программного окружения для разработки функций автоматизации. Злоумышленник может как собрать и украсть конфиденциальную информацию, так и закрепиться в системе и использовать ее для управления другими производственными частями предприятия, вплоть до остановки промышленных процессов;
- заражение трояном устройств IIoT. Для разработки прошивок для таких устройств используются открытые библиотеки и репозитории, где не всегда реализован контроль целостности программного обеспечения (ПО) и возможно заражение ПО вредоносным кодом;
- уязвимости в ПО мобильного интерфейса управления «человек-машина» – mobile HMI;
- искажение данных на системах управления производством (MES) для вызова сбоя в производственном процессе, например, путем изменения параметров на индикаторы дефектности или ввода параметров вне ожидаемого списка (out-of-bound), что приведет к отказу в обслуживании и заблокирует производство;
- использование уязвимой или вредоносной логики автоматизации в сложной производственной машине. Введенные в логику ошибки программирования сложные системы могут использоваться злоумышленниками для нарушения производственного процесса, если они уже получили доступ к промышленной сети.

По оценкам [4] в 2019 годах на промышленные компании пришлось 10% кибератак среди юридических лиц (рис. 1), что создает недопустимую иллюзию отсутствия у злоумышленников интереса к сфере АСУ.

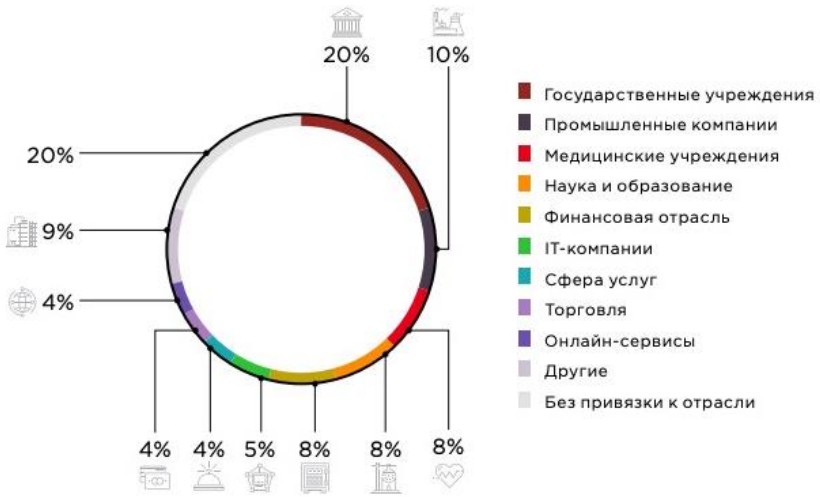

Рис. 1. Распределение кибератак в 2019 г. в сферах деятельности юридических лиц

Информация по-прежнему представляет высокую ценность для киберпреступников. Доля атак, направленных на получение данных, в 2019 г. составила 60% от общего числа атак на юридических. Но вектор атак меняется. В 2018 г. на долю промышленных систем приходилось 4% атак, то есть за один год их доля увеличилась в 2,5 раза. Представленное на рис 1 распределение связано с пока незначительным объемом АСУ ТП, подключенных к Интернет. По мере цифровизации доля АСУ ТП, входящих в СПАУ, в Интернете будет расти, что увеличивает возможность наступления неблагоприятных последствий в КИИ вследствие «цифрового неравенства» его составляющих.

2 Цифровое неравенство

К причинам цифрового неравенства можно отнести:

- отсутствие устоявшейся и непротиворечивой терминологии в области информационных и автоматизированных систем, систем корпоративного и технологического управления;
- невключение в систему обязательных требований к ряду автоматизированных систем управления требований по информационной безопасности;
- необоснованную, в ряде случаев, свободу маневра операторов между системами корпоративного и технологического управления для уклонения от исполнения обязательных требований. Данное обстоятельство наиболее отчетливо проявилось в процессе категорирования объектов КИИ, на что неоднократно указывала ФСТЭК России.

В части терминологии обратим внимание на следующие определения.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения).

Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон «Об информации, информационных технологиях и о защите информации».

Информационно-телекоммуникационная сеть (ИТКС) - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (Федеральный закон «Об информации, информационных технологиях и о защите информации».

Автоматизированная система управления (АСУ) - комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия (по смыслу ГОСТ 24.104-85. Межгосударственный стандарт. Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования).

Система промышленной автоматизации и управления (контроля, СПАУ) - совокупность персонала, аппаратного и программного обеспечений и политик, задействованных в функционировании промышленного процесса и способных влиять или воздействовать иным образом на его защищенное, безопасное и надежное функционирование (ГОСТ Р МЭК 62443-3-3-2016. Национальный стандарт РФ. Сети промышленной коммуникации. Безопасность сетей и систем. Ч. 3-3. Требования к системной безопасности и уровни безопасности).

В части уточнения терминологии имеет смысл обратиться также к ранее упомянутой «Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», в соответствии с которой:

- информационное общество - общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан;
- информационное пространство - совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры;
- экосистема цифровой экономики - партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, ин-формационных систем органов государственной власти Российской Федерации, организаций и граждан».

Исходя из смысла приведенных определений, к цифровым системам корпоративного управления (далее – ЦСКУ) отнесем системы, в которых объектами конечного воздействия данных является

человек, коллектив и порождаемые ими действия. К цифровым системам технологического управления (далее – ЦСТУ) - соответственно системы, в которых объектами конечного воздействия данных является устройство или совокупность устройств, порождающих действия без участия человека.

Такое допущение позволяет рассматривать объекты информационного общества, цифровой экономики, КИИ в виде двух видов укрупненных автоматизированных систем:

- ЦСКУ, как систем, реализующих функции административного управления, управления предприятием, производством, запасами, ресурсами и т.п.;
- ЦСТУ, как систем, осуществляющих управление технологическими процессами производства продукции и оказания услуг, осуществления денежных операций, технического обслуживания, проведения экспериментов, функционирования IoT и т.п.

Исторически сложилось так, что функционирование ЦСКУ рассматривалось в неразрывной связи с безопасностью информации. Поэтому существуют развитая нормативно-методическая база и опыт обеспечения информационной безопасности ЦСКУ, их аттестации и поддержания заданного уровня функционального состояния.

Применительно к ЦСТУ такую базу и опыт можно выделить, пожалуй, только в сфере финансовых организаций, защита информации в которых регламентируется, в частности, ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», распорядительными документами и стандартами Банка России (например, Положение от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиентов», стандарты серии СТО БР ИББС-1.х «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»).

Неоспоримо, что в любой цифровой системе управления изменение состояния управляемого объекта происходит вследствие информационного воздействия. Но также неоспоримо, что и сама информация подвергается изменению в результате протекания функциональных процессов. Следуя ГОСТ Р ИСО 15704-2008 «Требования к стандартным архитектурам и методологиям предприятия», это позволяет представить общую для ЦСКУ и ЦСТУ цифровую архитектуру в составе пяти уровней (рис. 2). В ней ЦСКУ занимают третий и четвертый уровни, а ЦСТУ могут охватывать уровни с нулевого до второго и далее вплоть до четвертого.

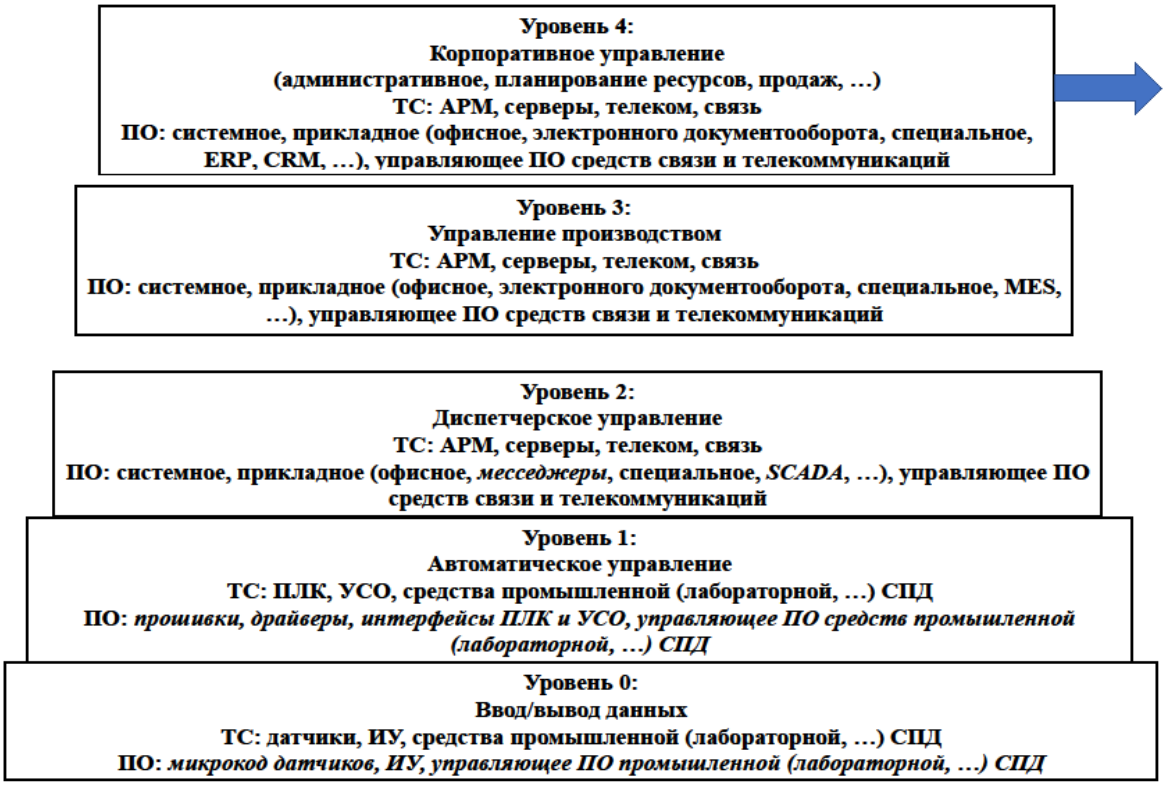

Рис. 2. Сегментированная структура АСУП и АСУТП

Структура интегрированной ЦСКиТУ представлена на рис.3.

Однако в системах технологического управления длительное время не уделялось должного внимания вопросам информационной безопасности, что привело к ряду крупных инцидентов. На то, что именно вследствие ускоренной интеграция ЦСКУ с трансформируемыми АСУ ТП возникает большинство инцидентов в ЦСКиТУ указывает анализ кибератак, в том числе пример, приведенный на рис. 4.

Повышенное внимание к обеспечению безопасности ЦСКиТУ является мировой тенденцией. Так, в частности, в 2019 году некоммерческий консорциум The Linux Foundation запустил проект ELISA (Enabling Linux In Safety Applications) [5]. Проект направлен на создание общего набора инструментов и процессов для создания и сертификации критически важных для безопасности приложений и систем на основе Linux, отказ которых может привести к человеческим жертвам, значительному материальному ущербу или ущербу окружающей среде, таких, например, как роботизированные устройства, медицинские устройства, интеллектуальные фабрики, транспортные системы и автономное вождение с использованием Linux и других.

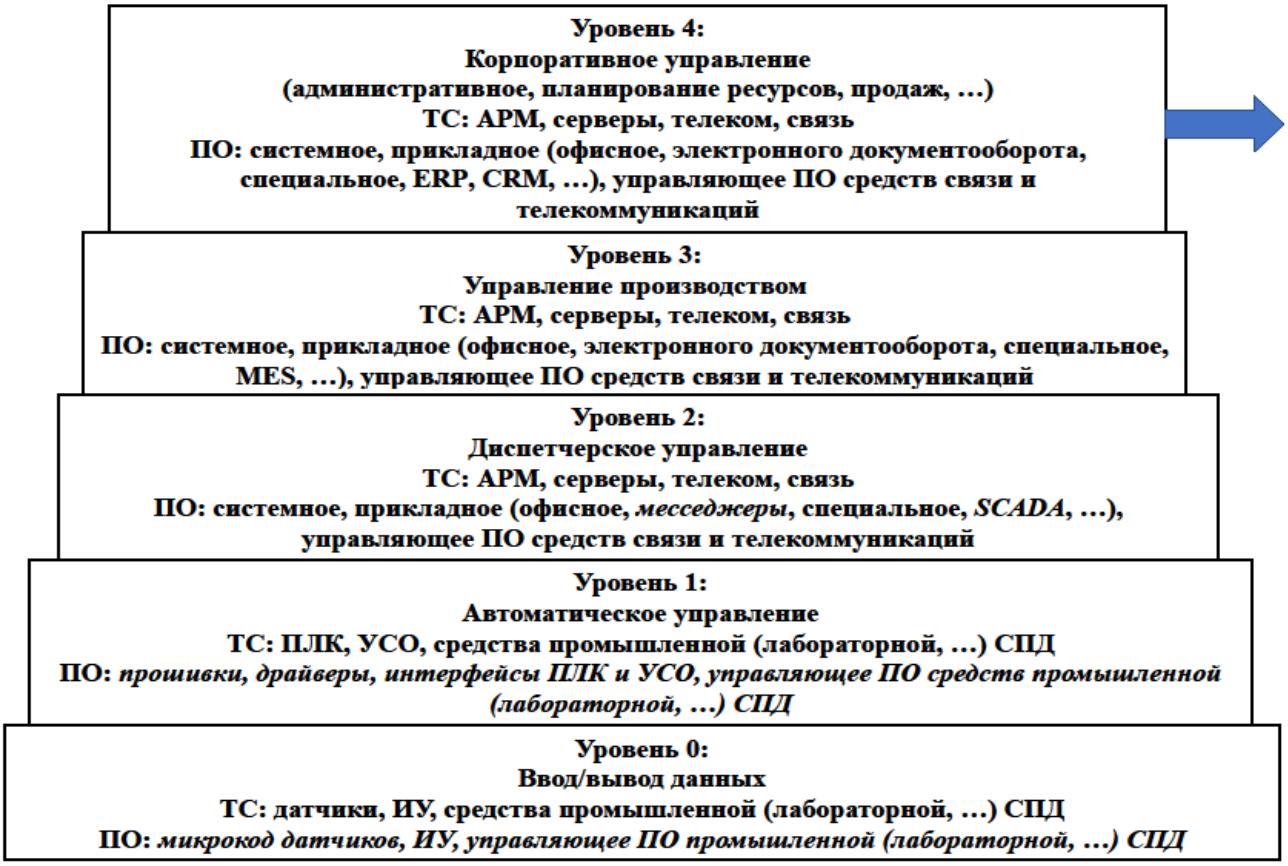

Рис. 3. Структура интегрированной ЦСКиТУ

Консорциум отмечает, что все основные отрасли, включая энергетику, медицину и автомобилестроение, хотят использовать Linux для приложений, требующих высокого уровня безопасности, поскольку это позволяет им быстрее выводить продукты на рынок и снижать риск критических ошибок проектирования. Проблема заключалась в отсутствии четкой документации и инструментов, необходимых для демонстрации того, что система на основе Linux соответствует требованиям безопасности для сертификации в гражданских областях. Поэтому консорциум проектом гражданской инфраструктурной платформы (CIP) стремится улучшить внедрение систем гражданской инфраструктуры на основе Linux с помощью программного обеспечения промышленного уровня и универсальной операционной системы, которая будет поддерживаться более десяти лет.

Рис. 4. Пример реализации кибератаки в ЦСКиТУ (рисунок: Павел Осинский. Презентация «Промышленная кибербезопасность. Инструменты»)

Как подчеркивается в [6], чтобы системе с высокими требованиями безопасности можно было доверять, она должна соответствовать целям функционирования и безопасности, включая то, как она реагирует на различные действия вроде ошибок пользователя и изменений среды. Разработчики должны показать, что их ПО соответствуют строгим требованиям к надежности, обеспечению качества, управлению рисками, процессу разработки и документации. Поскольку не существует четкого метода сертификации Linux, компаниям бывает сложно продемонстрировать, что их Linux-система отвечает этим требованиям безопасности. Поэтому ELISA взаимодействует с сертификационными органами и органами стандартизации в различных отраслях, что позволит установить, как Linux можно использовать в качестве компонента в критически важных для безопасности системах. В рамках проекта должен быть определен и поддерживаться общий набор элементов, процессов и инструментов, которые могут быть включены в основанные на Linux критические для безопасности системы, подлежащие сертификации по безопасности.

Проект ELISA также имеет дополнительные цели, в числе которых:

- разработка справочной информации и вариантов использования;
- обучение сообщества разработчиков ПО с открытым исходным кодом передовым методам безопасной разработки и ознакомление сообщества специалистов по безопасности с принципами открытой разработки;
- обеспечение постоянной обратной связи с сообществом разработчиков открытого ПО для улучшения рабочих процессов и автоматизации оценки и обеспечения качества;
- поддержка участников с помощью мониторинга инцидентов и опасностей в компонентах, относящихся к их системам, и обеспечение передовых методик взаимодействия с группами реагирования участников.

Изложенные консорциумом цели, мотивы и принципы близки автору, руководившему и принимавшему непосредственное участие в разработке российской защищенной аппаратно-программной платформы «Синтез-АПП» на основе Linux [7]. Несомненным является то, что следование им обеспечивает высокую оперативность и качество разработки безопасного ПО.

3 Трансформация приоритетов критериев безопасности

Увеличение числа инцидентов в трансформируемым АСУ ТП повлекло повышение активности регуляторов во всем мире. В частности, с 2014 года, когда ФСТЭК России приказом № 31 утвердил «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», стала активно развиваться нормативно-методическая база обеспечения безопасности критической информационной инфраструктуры РФ.

Согласно Федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» безопасность КИИ - это состояние защищенности, обеспечивающее устойчивое функционирование КИИ при проведении в отношении ее компьютерных атак. То есть, функционирование объектов КИИ зависит от компьютерной, а не от информационной безопасности? Или эти термины являются синонимами? И если да, то это полный перечень?

Как показано в [8], один и тот же смысл зачастую может вкладываться в термины компьютерная безопасность, информационная безопасность, безопасность информационных технологий, кибербезопасность и кибербезопасность, но на восприятие будет влиять тот контекст, который в данный момент более понятен простому пользователю.

Такого рода терминологическая неопределенность неприемлема, так как создает дополнительные трудности и так в непростом общении специалистов в области функциональной безопасности, информационной безопасности к которым теперь добавляются «кибербезопасники».

Наряду с нормативной базой ФСТЭК России и ФСБ России, в ведомствах и других структурах развивается своя нормативная база, в которой присутствуют уже упомянутые термины.

Например, в СТО РЖД 08.021-2015 (Устройства железнодорожной автоматики и телемеханики. Порядок разработки, испытаний и постановки на производство) термин информационная безопасность (железнодорожной автоматики и телемеханики) определен как свойство аппаратно-программного средства железнодорожной автоматики, связанного с безопасностью движения поездов, выполнять требуемые функции безопасности в течение заданного периода времени с обеспечением защиты от несанкционированного доступа к управляющей и контрольной информации и отсутствием недекларированных возможностей программного обеспечения.

В СТО РЖД 02.049-2014 (Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия) термину киберзащищенность ПО АСУ ТП дано следующее определение. Киберзащищенность ПО АСУ ТП - это устойчивое и безопасное состояние ПО, позволяющее выполнять предусмотренные задачи в условиях деструктивных воздействий с использованием инфраструктуры или элементов киберпространства, направленных на нарушение функционирования АСУ ТП, нарушение без-опасности движения или причинения ущерба объектам, находящимся под контролем и управлением АСУ ТП (Примечание - Киберпространство - среда информационного взаимодействия и обмена данными, реализуемая в компьютерных сетях и сетях связи. Элементами киберпространства являются сервера, компьютеры, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети).

В стандарте ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity, входящем в серию стандартов по безопасности информационных технологий, терминологические границы установлены следующим образом:

«Кибербезопасность: Состояние защищенности от физического, социального, духовного, финансового, политического, эмоционального, оккупационного, психологического, образовательного и других типов и последствий неудачи, повреждения, ошибки, происшествия, вреда и других событий в киберпространстве, которые признаны нежелательными (Примечания: 1 Такое состояние может быть выражено формой защищенности от события или воздействия, которое вызывает утрату здоровья или экономические потери. Оно может включать защит от людей и ресурсов. 2 Безопасность в целом также определяют как состояние уверенности в том, что негативные эффекты не будут вызваны некоторыми агентами при соблюдении определенных условий.

Информационная безопасность, безопасность киберпространства: Сохранение конфиденциальности, целостности и доступности информации в киберпространстве (Примечания: 1. Кроме того, такие свойства, как аутентичность, ответственность, невозможность отказа от авторства и надежность также могут быть вовлечены. 2 Адаптировано из определения информационной безопасности стандарта ISO/IEC 27000:2009).

Киберпространство: Комплексная среда, являющаяся результатом взаимодействия людей, ПО и услуг в Интернете посредством технологических устройств и сетей, к ним присоединенных, которая не существует в физической форме.

Интернет-безопасность: Состояние защищенности от физического, социального, духовного, финансового, политического, эмоционального, оккупационного, психологического, образовательного и других типов и последствий неудачи, повреждения, ошибки, происшествия, вреда и других событий в киберпространстве, которые признаны нежелательными.

Интернет-безопасность: Сохранение конфиденциальности, целостности и доступности информации в сети Интернет».

То есть, даже в одном документе даны идентичные определения терминам кибербезопасность и интернет-безопасность в одном случае, информационная безопасность и интернет-безопасность в другом. Стандарт ISO/IEC 27032:2012 объясняет новый термин направленным на улучшение состояния именно киберпространства за счет извлечения уникальных аспектов киберактивности и их зависимости от остальных областей безопасности, к которым отнесены, для примера, информационная, сетевая и интернет безопасность, а также защита ключевой информационной структуры (рис. 5). Кибербезопасность, в данном случае, выделяет проблемы безопасности, не покрытые существующей информационной, сетевой, интернет и информационно-коммуникационной технологиями из-за брешей между указанными областями, а также благодаря дефициту общения между организациями и поставщиками услуг в киберпространстве.

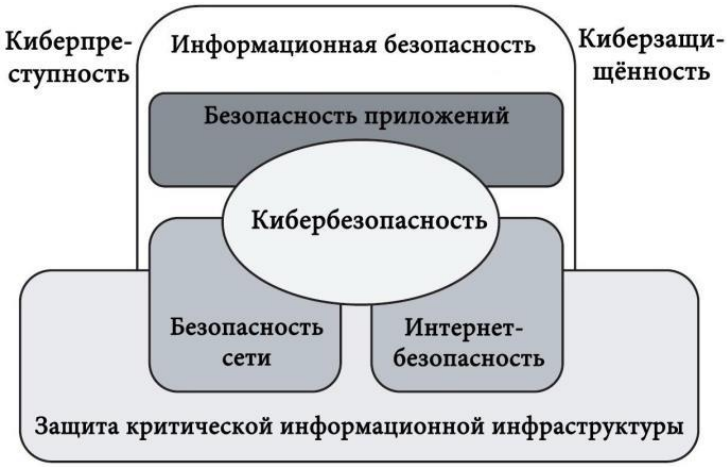

Рис. 5. Связи между кибербезопасностью и другими областями безопасности (ISO/IEC 27032:2012)

Проявляя заботу об улучшении киберпространства, следует учитывать и неявно присутствующие в описанных областях сферы безопасности социальных сетей и инженерно-технических систем. Социальные сети представлены в киберпространстве миллиардами пользовательских устройств, являющихся полноценными средствами вычислительной техники и потенциальными участниками бот-сетей. Системы инженерно-технической защиты присутствуют в киберпространстве в виде датчиков, контролеров, исполнительных устройств систем контроля и управления доступом, охраны и сигнализации, видеокамерами систем видеонаблюдения и т.п.

Анализ текущего состояния нормативных документов приводит к выводу, что идет активный поиск базы, способной интегрировать, на первый взгляд, ортогональные системы требований. Однако, как уже упоминалось выше, в распределенных ЦСТУ все виды безопасности (функциональной, инженерно-технической и др.) коррелированы с информационной безопасностью, что требует четкого и непротиворечивого установления причинно-следственных связей функциональных и информационных процессов, разработки адекватных моделей угроз, формирования требований к системам защиты и их реализации. Кибербезопасность не может и не должна рассматриваться отдельно.

Требования к кибербезопасности ЦСКУ и ЦСТУ во многом совпадают, так как совпадают направленные на них угрозы и способы их реализации. Стратегии безопасности ЦСКУ как правило строятся вокруг защиты информации и опираются на принцип К-Ц-Д: конфиденциальность, целостность и доступность информации, так как именно информация рассматривается в качестве основного актива. В ЦСТУ на первый план выходят устойчивость, оперативность, непрерывность управления, поэтому их защита подразумевает обеспечение доступности, целостности и конфиденциальности данных, т.е. принцип защиты трансформируется к виду Д-Ц-К (рис. 6). Из-за этой особенности промышленных систем даже лучшее решение для обеспечения кибербезопасности является бесполезным, если ставит под угрозу непрерывность технологических процессов.

Рис. 6. Трансформация приоритетов критериев безопасности (рисунок: [9])

В ЦСКиТУ, как интегрированных системах управления, цели кибератак могут варьироваться от нарушения информационной безопасности до нарушения технологических процессов, способных повлечь не только остановку промышленного комплекса в целом, но и возникновение катастроф. Поэтому, в ЦСКиТУ, относимых, например, к значимым объектам КИИ, для недопущения нарушения или прерывания их деятельности можно пожертвовать приоритетом конфиденциальности информации в системе критериев.

4 Трансформация технологического обеспечения безопасности

Цифровое неравенство ЦСКУ и ЦСТУ проявилось также в разной обеспеченности средствами защиты. Так, например, известно достаточное число сертифицированных операционных систем и программных платформ, обеспечивающих защиту ЦСКУ. В то же время их активное применение в процессе ускоренной цифровой трансформации ЦСТУ повлекло возникновение значительного числа известных инцидентов кибербезопасности ЦСТУ. Данное обстоятельство послужило катализатором развития технологической базы обеспечения безопасности ЦСКиТУ.

Так, в частности, ФСТЭК России утверждены Требованиями безопасности информации к операционным системам, которыми определены три типа операционных систем:

- тип «А» - операционная система общего назначения (операционная система, предназначенная для функционирования средств вычислительной техники общего назначения (автоматизированные рабочие места, серверы, смартфоны, планшеты, телефоны и иные);
- тип «Б» - встраиваемая операционная система (операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач);
- тип «В» - операционная система реального времени – операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Такое решение обеспечивает применение на каждом уровне ЦСКиТУ того типа ОС, который наиболее адаптирован к требованиям безопасности для данного уровня.

Разрабатываются решения по криптографической защите каналов связи на нижних уровнях ЦСКиТУ, образуемых между программируемыми логическими контроллерами (PLC), промышленными контроллерами автоматизации (PAC), терминалами (RTU), интеллектуальными устройствами (IED), оконечным оборудованием (сенсоры, датчики, счетчики, различные исполнительные устройства) [10].

Активно создаются комплексные решения обеспечения безопасности ЦСКиТУ, например, иллюстрируемые на рис 7, 8.

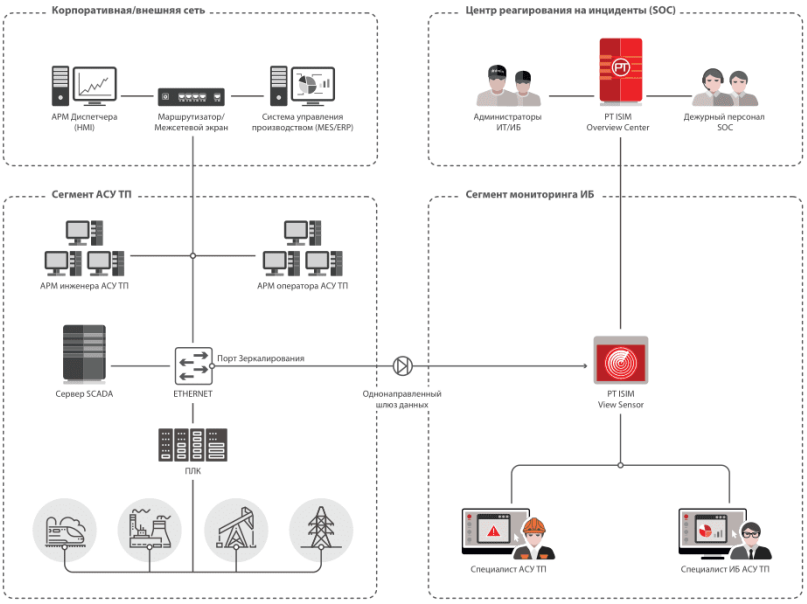

Рис. 7. Комплексное решение по защите ЦСКиТУ (вариант, источник: https://www.ptsecurity.com/ru-ru/products/isim/)

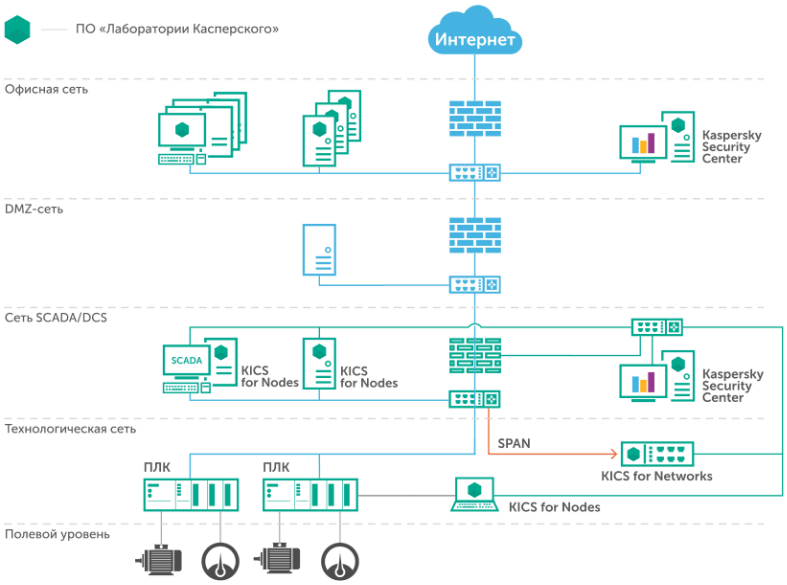

Рис. 6. Комплексное решение по защите ЦСКиТУ (вариант, источник: https://ics.kaspersky.ru/resources/#solution)

Общей тенденцией противостояния киберпреступности становится создание киберполигонов и иных ресурсов, обеспечивающих тестирование решений безопасности. Ресурсы Интернета позволяют обращаться к лучшим практикам, независимо от стран их происхождения (ELISA и др., например, некоммерческая организация The European Network for Cyber Security (ENCS, https://encs.eu/), объединяющая представителей компаний энергетической инфраструктуры в Европе, выпускает документы по кибербезопасности в энергетики, включая готовые требования кибербезопасности к элементам систем автоматизации, программы тестирования на основании этих требований, предоставляет ресурсы для проведения тестирования).

Заключение

Цифровизация выявила многие проблемы обеспечения безопасности информационного пространства, открыв «доступ» киберугрозам в АСУ ТП и на нижние уровни интегрированных ЦСКиТУ. Это активизировало процессы, направленные на преодоление цифрового неравенства между

ЦСКУ и ЦСТУ, развитие нормативно-правовой базы, технологической базы обеспечения их кибербезопасности.

В то же время одномоментно выровнять защищенность ЦСКУ и ЦСТУ не представляется возможным в силу накопившегося неравенства в номенклатуре средств защиты информации, например. Это же касается подготовки кадров, которую необходимо перестраивать, ориентировать на подготовку специалистов, понимающих процессы, протекающие в интегрированных ЦСКиТУ, значительно более сложные, чем процессы, рассматриваемые отдельно в ЦСКУ и отдельно в ЦСТУ. Неравенство просматривается также и в области терминологии, когда одни и те же термины могут толковаться по-разному, и в формулировке требований по кибербезопасности.

Гармонизация требований кибербезопасности интегрированных ЦСКиТУ направлена на повышение уровня взаимопонимания специалистов по обеспечению информационной безопасности и обеспечению функционирования ЦСКиТУ, что позитивно скажется на противодействие общих для них угроз, исходящих из открытого информационного пространства.

Литература

1. *Михалевич И.Ф.* Проблема цифрового неравенства автоматизированных систем корпоративного и технологического управления // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 3. - С. 43-47
2. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты. Источник: https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review. (доступ 23.05.2020).
3. Атаки на производственные системы и IIoT: основные векторы и рекомендации по защите Источник: https://www.angaratech.ru/press-center/novosti/ataki-na-proizvodstvennye-sistemy-i-iiot-osnovnye-vektory-i-rekomendatsii-po-zashchite_1096/?utm_source=facebook&utm_medium=social&utm_campaign=promo (доступ 23.05.2020).
4. Актуальные киберугрозы: итоги 2019 года. Источник: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/ (доступ 23.05.2020).
5. The Linux Foundation Launches ELISA Project Enabling Linux In Safety-Critical Systems. Источник: https://www.linuxfoundation.org/press-release/2019/02/the-linux-foundation-launches-elisa-project-enabling-linux-in-safety-critical-systems/ (доступ 24.05.2020).
6. Advancing Open Source Safety-Critical Systems. Источник: https://elisa.tech/ (доступ 24.05.2020).
7. *Михалевич И.Ф.* Теоретические и практические аспекты создания отечественных защищенных аппаратно-программных платформ для критической информационной инфраструктуры Российской Федерации // Интеллектуальные системы. Теория и приложения. - Том. 22, вып. 3, 2018. С. 7-17.
8. Schatz, Daniel; Bashroush, Rabih; and Wall, Julie (2017) "Towards a More Representative Definition of Cyber Security," Journal of Digital Forensics, Security and Law: Vol. 12 : No. 2 , Article 8.
9. Промышленная кибербезопасность. Источник: https://media.kaspersky.com/pdf/Kaspersky_Industrial_CyberSecurity_solution_descr.pdf. (доступ 24.05.2020).
10. Индустриальный криптографический модуль ViPNet SIES Core 2. Источник: https://infotecs.ru/product/vipnet-sies-core.html#soft (доступ 26.05.2020).