УДК 005

DOI: 10.37468/2307-1400-2020-3-51-58

БУЙНЕВИЧ МИХАИЛ ВИКТОРОВИЧ,
ИЗРАИЛОВ КОНСТАНТИН ЕВГЕНЬЕВИЧ,
ПОКУСОВ ВИКТОР ВЛАДИМИРОВИЧ,
ЯРОШЕНКО АЛЕКСАНДР ЮРЬЕВИЧ

ОСНОВНЫЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ АРХИТЕКТУРЫ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ

АННОТАЦИЯ

Рассматривается проблема построения единой систем защиты на базе качественно различных подсистем, ответственных за свои классы атак. Предложены пять следующих основных принципов проектирования архитектур таких систем: искусственность декомпозиции, необходимость и достаточность подсистем, структурная инвариантность, универсализация взаимодействия, единое информационное пространство. Приведены графические схемы примеров применения принципов.

Ключевые слова: система защиты, архитектура, принципы проектирования.

BUINEVICH M. V.,
IZRAILOV K. E.,
POKUSOV V. V.,
YAROSHENKO A. YU.

MAIN PRINCIPLES OF DESIGNING THE MODERN PROTECTION SYSTEMS ARCHITECTURE

ABSTRACT

The problem of building a unified protection system based on qualitatively different subsystems responsible for their classes of attacks is considered. The following five basic principles of designing architectures of such systems are proposed: artificial decomposition, necessity and sufficiency of subsystems, structural invariance, universalization of interaction, and a single information space. Graphical diagrams of examples of application of the principles are given.

Keywords: protection system, architecture, design principles.

Введение

Для любой организации в современном мире воздействие атак на ее ресурсы является существенной проблемой, актуальность которой из года в год только возрастает; для противодействия им создаются соответствующие системы защиты [1]. По причине же многообразия атак (программно-математических, перемещения, природных, технических и др.) системы защиты вынужденно строятся из целого набора специализированных подсистем, каждая их которых ответственна за свой класс (канал). Однако из этого и следует одно из основных противоречий предметной области. Совместная работа подсистем, построенных на различной базе, но в рамках единой системы, как правило, имеет меньшую суммарную эффективность защиты [2, 3] – подсистемы начинают конфликтовать, снижая результативность; противодействие атакам, состоящим из нескольких классов, требует дополнительного времени для связывания их надсистемой в единый вектор [4], снижая оперативность; методы и средства согласования вза-

имодействия подсистем требуют дополнительных накладных расходов (как программно-аппаратных, так и человеческих), что приводит к росту ресурсоемкости. И, как было показано неоднократно ранее авторами [5, 6, 7], разрешение противоречия может быть обеспечено только на этапе проектирования системы защиты путем синтеза ее научно-обоснованной и практически-состоятельной архитектуры (как, например, в [8]), которая как раз и закладывает фундамент потенциальной эффективности [9, 10] (в данном контексте под архитектурой системы понимается состав ее подсистем, а также организация их информационно-технического взаимодействия). Поэтому этот вопрос является крайне принципиальным и требует своего осмысления.

Постулировать основные принципы проектирования архитектуры современных систем защиты и предполагается в настоящей статье.

Принципы проектирования

Используя богатый опыт в анализе проблемных вопросов систем защиты информации [11, 12, 13], а также в оценке их результирующей эффективности [14], были сформулированы следующие пять принципов, следование которым, по мнению авторов, позволит синтезировать архитектуру систем защиты информационных ресурсов, избавленную от множества внутренних противоречий, присутствующих в эволюционно построенных (т.е. постепенно, без заранее спроектированной структуры).

Принцип 1. Искусственность декомпозиции (целенаправленность)

Большинство систем защиты создавалось, адаптируясь к изменяемому миру – по мере возникновения новых классов угроз, появления средств защиты, формирования требований к работе. Тем самым создание архитектур систем представляло собой эволюционный процесс. При этом входящие в состав подсистемы формировались из уже существующих (независимых) элементов, что негативно сказывалось на результирующей эффективности системы защиты, поскольку элементы изначально создавались для достижения собственных целей, которые после включения в состав единой системы оказывались несогласованными. Так, например, подсистема контроля и управления доступом будет стремиться не допустить на территорию организации лиц без пропуска, а в случае обнаружения подсистемой пожарной сигнализации очага возгорания и автоматического вызова «внешней» пожарной бригады, последняя не сможет пройти через проходную (по крайне мере, потребуется время для предоставления им доступа) – явный диссинергетический эффект [15].

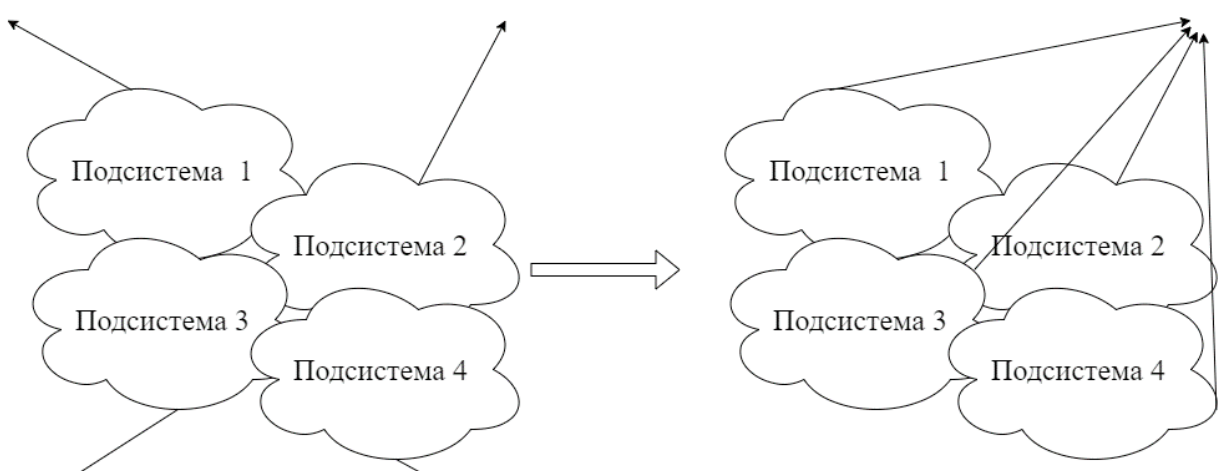
Его предотвращение приводит к первому принципу построения системы защиты – *искусственной декомпозиции на подсистемы с учетом общей целенаправленности*. В результате архитектура будет изначально создаваться так, чтобы гармонизировать частные цели подсистем в направлении основной цели системы [16, 17, 18, 19]. Яркий пример – создание «продвинутых» систем охранно-пожарной сигнализации.

Представим применение принципа с помощь следующей схемы (Рис. 1).

Согласно схеме, изначально (см. рис. 1а) каждая из подсистем имеет свою «изолированную» цель, поскольку создавалась независимо от других. В случае применения первого принципа (см. рис. 1б) все подсистемы «работают» на общую цель.

Принцип 2. Необходимость и достаточность подсистем

Создание архитектуры системы защиты из набора уже имеющихся подсистем имеет два существенных недостатка. Во-первых, используемые подсистемы могут иметь перекрывающийся функционал, как излишне дублируя решаемые задачи, так и мешая тем самым друг другу. Например, достаточно часто задача обновления программного обеспечения серверов ложится как на подсистему сетевой безопасности, так и внутренней технической поддержки. Во-вторых, может сложиться ситуация, когда существующие подсистемы будут выполнять только часть требуемых задач, а создание новой ради решения оставшихся задач окажется нецелесообразным. Например, подсистема контроля и управления доступом не ведет запись заезжающих на территорию автомобилей (а только управляет поднятием шлагбаума), что не позволит в последствие сопоставить архивы событий при возникновении инцидента. Препят-



а) б)

Рисунок 1 – Пример создания систем защиты:
а) эволюционный процесс; б) целенаправленный процесс

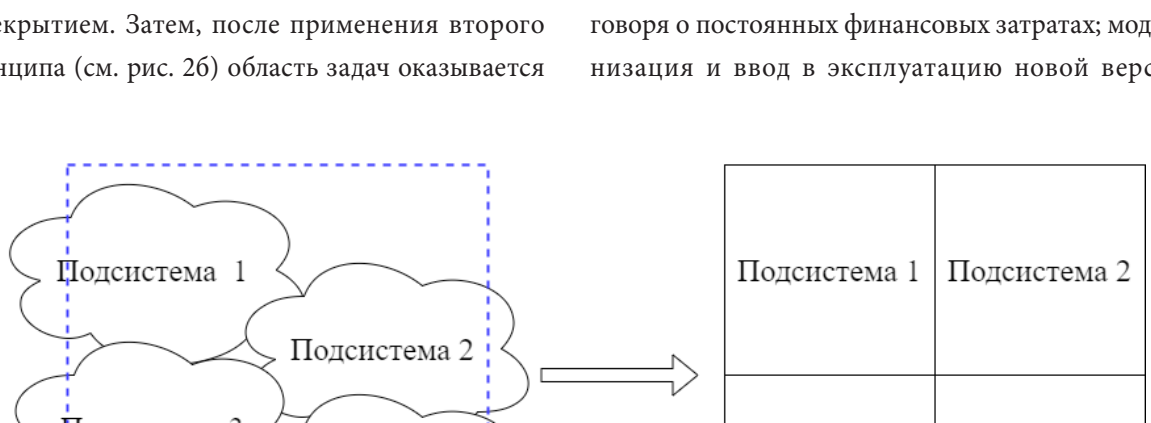
ствование дублированию и коллизиям возможно с помощью второго принципа построения системы защиты – *необходимости и достаточности деления на подсистемы* [20, 21]. Тем самым все множество подсистем перекроет все необходимые задачи, а каждая из подсистем не будет «залезать» в зону ответственности другой.

Представим применение второго принципа с помощь следующей схемы (Рис. 2).

Согласно схеме, изначально (см. рис. 2а) область задач (пунктиром) покрыта подсистемами не полностью или избыточно, а также с взаимным перекрытием. Затем, после применения второго принципа (см. рис. 2б) область задач оказывается полностью «покрыта» функционалом подсистем без их взаимного пересечения.

Принцип 3. Структурная инвариантность

Развитие современного мира, и в особенности повсеместное внедрение все новых IT-решений, приводит к постоянному изменению условий проведения старых атак, а также к появлению качественно новых. Все это требует как адаптации существующих механизмов и подсистем защиты, так и создания новых. При этом постоянные перестройки архитектуры их единой системы, очевидно, будет крайне негативным вариантом – не говоря о постоянных финансовых затратах; модернизация и ввод в эксплуатацию новой версии



а) б)

Рисунок 2 – Пример проектирования архитектуры из набора подсистем:
а) существующих; б) необходимых и достаточных

такой архитектуры попросту может не успевать за эволюционированием атакующих воздействий. Например, появление в организациях киберфизических устройств, полностью управляемых искусственным интеллектом (по аналогии с развитием беспилотных автомобилей в концепции Умного города), приведет и к новому классу атак, направленному на интеллектуальный центр управления. Создание же и внедрение в работающую архитектуру новой подсистемы защиты, а также ее согласование с остальными подсистемами, может оказаться невозможным и потребует частичного перестроения всей системы. Исходя из этого, имеет смысл изначально создавать такую архитектуру (и, следовательно, производить деление на подсистемы), которая бы оказывалась неизменной во времени – т.е. не требовала качественных перестроений при возникновении новых задач. Это соображение приводит к третьему принципу – *структурной инвариантности архитектуры системы защиты* [22, 23]. Учет принципа позволит расширять набор механизмов защиты от атак, осуществляя параметрический, но не структурный синтез новой системы.

Представим применение третьего принципа с помощь следующей схемы (Рис. 3).

Согласно схеме, изначально (см. рис. 3а) каждая из четырех подсистем отражает собственный класс атак. После появления нового класса (см. рис. 3б) «мощность» Подсистемы 4 (в смысле объема решаемых ею задач) возросла для дополнительного противодействия Атакам класса 5; при этом в систему защиты внесены параметрические (объем задач), но не структурные (количество подсистем) изменения.

Принцип 4. Универсализация взаимодействия

Необходимость совместной работы множества подсистем требует от них постоянного информационно-технического взаимодействия. Качественная же различность подсистем ведет к тому, что используемые ими информационные объекты, а также логика обмена последними, не позволяют их применить для полноценного взаимодействия, однозначно понятного всем его участникам. Например, в подсистеме контроля и управления доступом можно предположить наличие таких объектов, как запрос на идентификацию посетителя, открытие турникета, незаконное

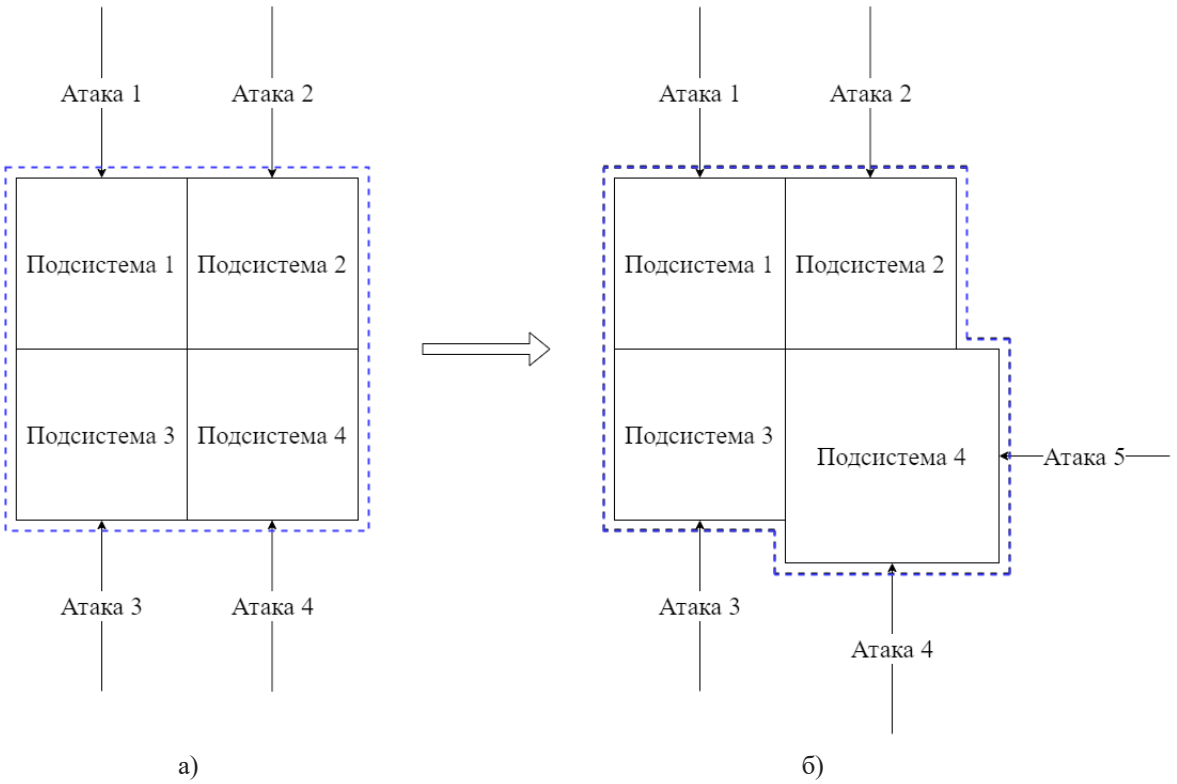


Рисунок 3 – Пример инвариантной архитектуры системы защиты в условиях: а) традиционных атак; б) нового класса атак (задач)

проникновение и др.; а для подсистемы пожарной сигнализации – повышение температуры в комнате, включение системы пожаротушения, вызов внешней пожарной бригады. Очевидно, что эти подсистемы с такими объектами обмена никогда не смогут «договориться» иначе как по уникальному протоколу. Таким образом, возникает необходимость в четвертом принципе – *универсализации взаимодействия подсистем защиты* [24]. Применение этого принципа позволит подсистемам общаться на базе единых объектов и используя понятную логику.

Представим применение четвертого принципа с помощь следующей схемы (Рис. 4).

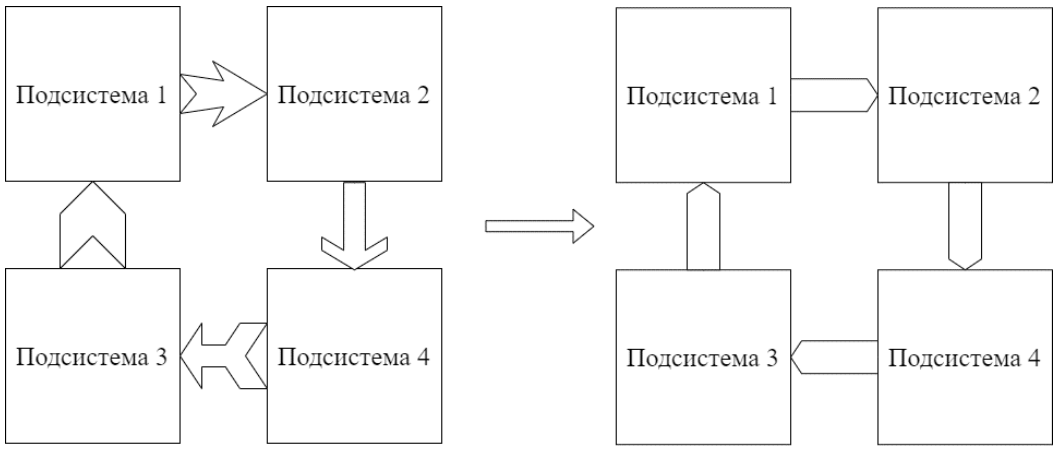


Рисунок 4 – Пример информационно-технического взаимодействия подсистем: а) уникального; б) универсального

Согласно схеме, изначально (см. рис. 4а) каждая из подсистем взаимодействует с другими, используя собственные уникальные формат и алгоритмы. После перевода всех взаимодействий на одну базу объектов обмена и логику (см. рис. 4б) будет реализован четвертый принцип.

Принцип 5. Единое информационное пространство

Помимо того, что подсистемы должны иметь универсальное взаимодействие друг с другом, они также должны обладать одинаковыми знаниями для принятия соответствующих решений. Таким образом, требуется синхронизация общей информации и унифицированный формат ее хранения. Так, обнаружение нового сценария атаки одной подсистемой должно стать известным и всем остальным, поскольку эта атака может оказаться частью вектора, действующего сразу через несколько зон ответственности подсистем. Например, диагностирование подсистемой контроля и доступа факта прохождения нарушителя путем клонирования электронного пропуска должно предупредить подсистемы сетевой безопасности и видеонаблюдения о высокой технической подготовки нарушителя и, следовательно, более высоких рисках взлома сети и нейтрализации видеокамер и датчиков сигнализации. Таким образом, возникает пятый принцип – *использование единого информационного пространства* [25-29]. Архитектура систем защиты, построенных с помощью этого принципа, позволит подсистемам использовать данные и функции из общего («расшаренного», от англ. to share) пространства – т.е. всегда находящиеся в актуализированном состоянии.

Представим применение пятого принципа с помощь следующей схемы (Рис. 5).

Согласно схеме, изначально (см. рис. 5а) каждая из подсистем содержит в себе собственную базу данных (возможно, с функциями их обработки), необходимых, в том числе, другим подсистемам. После перевода всех подсистем на единое информационное пространство (см. рис. 5б) они начинают общаться именно с ним, как с полномочным представителем баз данных всех подсистем.

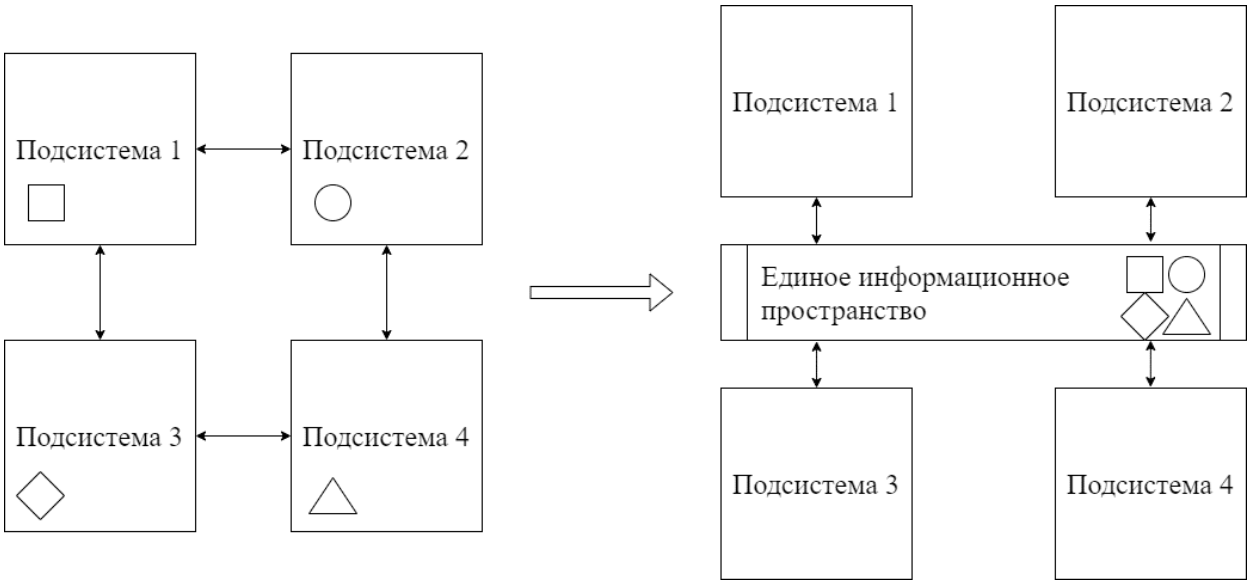


Рисунок 5 – Пример организации информационного пространства подсистем: а) собственного; б) единого

Выводы

Анализ проблемных вопросов современных систем защиты, а также богатый авторский опыт, позволили обоснованно предложить пять принципов построения таких систем. Принципы оказывают непосредственное влияние как на состав подсистем (включая решаемые ими задачи), так и на их взаимодействие. Применение одновременно всех принципов является достаточно сложной задачей, как с научной, так и с технической стороны. Тем не менее, перспективное направление их реализации авторами видится в следующем. Во-первых, это синтез состава подсистем с использованием категориального деления, что позволит соблюсти первые три принципа. А, во-вторых – организация универсального протокола (как совокупности объектов обмена и его логики) [30] информационно-технического взаимодействия между ними, что приведет к соблюдению последних двух принципов. Дальнейшим направлением исследований должна стать выработка рекомендаций для более точного соответствия реализаций архитектуры разрабатываемых систем защиты каждому из описанных принципов ее проектирования.

Список литературы

1. *Дорошенко А.В.* Проблемы организации защиты данных в информационных системах организаций // Экономическая безопасность государства как один из важнейших факторов стратегического развития экономики приднестровской молдавской республики: материалы Международной научно-практической конференции / Отв. ред. Н.Н. Смоленский, И.В. Толмачева, 2017. – С. 166-169.

2. *Израилов К.Е., Покусов В.В.* Актуальные вопросы взаимодействия элементов комплексных систем защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей: в 4-х томах / Под редакцией С.В. Бачевского, 2017. – С. 255-260.

3. *Буйневич М.В., Покусов В.В., Израилов К.Е.* Эффекты взаимодействия обеспечивающих служб предприятия информационного сервиса (на примере службы пожарной безопасности) // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2018. – № 4. – С. 48-55.

4. *Бирюков А.А., Израилов К.Е.* Сравнительный анализ моделей угроз информационной безопасности в интересах применимости для многоэтапных схем атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): сборник научных статей VI Международной научно-технической и научно-

методической конференции. В 4-х томах / Под редакцией С.В. Бачевского, 2017. – С. 108-112.

5. *Покусов В.В.* Особенности взаимодействия служб обеспечения функционирования информационной системы // Информатизация и связь. – 2018. – № 5. – С. 51-56.

6. *Буйневич М.В., Покусов В.В., Ярошенко А.Ю., Хорошенко С.В.* Категориальный подход в приложении к синтезу архитектуры интегрированной системы обеспечения безопасности информации // Проблемы управления рисками в техносфере. – 2017. – № 4 (44). – С. 95-102.

7. *Буйневич М.В., Киричок А.И.* Подход к реализации комплексной АСУ архитектурным и наружным освещением Москвы // Автоматизация в промышленности. – 2013. – № 11. – С. 42-46.

8. *Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A.* Software defined internet of things: cyber antifragility and vulnerability forecast // Application of Information and Communication Technologies (AICT-2017). – 2017. – PP. 293-297.

9. *Покусов В.В.* Оценка эффективности системы обеспечения ИБ. Часть 1. Показатели и модели представления // Защита информации. Инсайд. – 2019. – № 2 (86). – С. 54-60.

10. *Покусов В.В.* Оценка эффективности системы обеспечения ИБ. Часть 2. Методика и результаты // Защита информации. Инсайд. – 2019. – № 3 (87). – . 64-72.

11. *Антюхов В.И., Сугак В.П., Ярошенко А.Ю., Остудин Н.В.* Моделирование процесса обеспечения безопасности информации в подразделениях МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: материалы VII Международной научно-практической конференции, 2015. – С. 71.

12. *Ярошенко А.Ю., Буйневич М.В.* Обоснование потребности в методике оценки качества и эффективности комплексной организационно-технической системы обеспечения безопасности информации в МЧС России // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2016. – № 4. – С. 57-62.

13. *Антюхов В.И., Остудин Н.В., Ярошенко А.Ю., Черных А.К.* Информационная потребность должностных лиц центров управления в кризисных ситуациях (ЦУКС) МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: материалы VII Международной научно-практической конференции, 2015. – С. 70-71.

14. *Ярошенко А.Ю., Буйневич М.В.* Обоснование потребности в методике оценки качества и эффективности комплексной организационно-технической системы обеспечения безопасности информации в МЧС России // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2016. – № 4. – С. 57-62.

15. *Покусов В.В.* Синергетические эффекты взаимодействия модулей системы обеспечения информационной безопасности // Информатизация и связь. – 2018. – № 3. – С. 61-67.

16. *Елкин В.И.* О декомпозиции управляемых систем на одномерные независимые системы // Моделирование, декомпозиция и оптимизация сложных динамических процессов. – 1999. – Т. 14. – № 1 (14). – С. 93-96.

17. *Гридин В.Н., Анисимов В.И.* Декомпозиция больших систем на основе описания переменных разделения в смешанном базисе // Информационные технологии в проектировании и производстве. – 2019. – № 4 (176). – С. 3-7.

18. *Витомский Е.В.* Принципы декомпозиции компьютерных систем по типам уязвимостей // Информационные технологии в проектировании и производстве. – 2005. – № 2. – С. 24-28.

19. *Сумин В.И., Кузнецова Л.Д., Колыхалин В.М.* Разработка информационных систем с декомпозицией систем управления на подсистемы // Качество в производственных и социально-экономических системах: сборник научных трудов 2-ой Международной научно-практической конференции, посвященной 50-летию Юго-Западного государственного университета: в 2-х томах / Ответственный редактор Павлов Е.В., 2014. – С. 350-353.

20. *Кузнецов В.* Необходимые и достаточные условия // Математика. Первое сентября. – 2013. – № 10. – С. 14-16.

21. *Аршинский В.Л., Аршинский Л.В., Бахвалов С.В.* Принципы необходимости и достаточности в систематизации программного обеспечения // Автоматизация и моделирование в проектировании и управлении. – 2019. – № 2 (4). – С. 18-24.

22. *Жукова Г.С.* Представление сложных систем на основе принципа инвариантности // Ученые записки Российского государственного социального университета. – 2010. – № 8 (84). – С. 23-26.

23. *Проскурников А.В., Якубович А.* Задача об инвариантности системы управления // Доклады Академии наук. – 2003. – Т. 389. – № 6. – С. 742-746.

24. *Чувиков Д.А.* Универсальные алгоритмы взаимодействия экспертной системы и системы имитационного моделирования // T-Comm: Телекоммуникации и транспорт. – 2017. – Т. 11. – № 4. – С. 34-40.

25. *Громов Ю.Ю., Ивановский М.А., Дидрих В.Е., Погонин В.А.* Принципы защиты информации полей единого информационного пространства // Промышленные АСУ и контроллеры. – 2010. – № 8. – С. 51-56.

26. *Сенченко П., Жуковский О., Гриценко Ю.* Принципы организации единого информационного пространства при разработке комплексов дистанционного управления технологическим процессом // Проблемы теории и практики управления. – 2018. – № 10. – С. 114-125.

27. *Зайцев А.Н.* Формирование внутренней структуры базы данных для организации единого информационного пространства // Морская радиоэлектроника. – 2019. – № 4 (70). – С. 18-21.

28. *Кузенбаев А.А., Байманкулов А.Т.* Применение системного подхода в моделировании единого информационного пространства // Теория и практика современной науки. – 2020. – № 3 (57). – С. 141-144.

29. *Крицкий А.В., Каргапольцев Д.С., Брусницын Д.Н., Скоринов С.В., Шабуров Д.П., Добразов А.Е.* Единое информационное пространство программно-аппаратных средств // Водоснабжение и санитарная техника. – 2015. – № 11. – С. 45-56.

30. *Покусов В.В.* Формат протокола универсального информационно-технического взаимодействия в системе обеспечения информационной безопасности «УИТВ-СОИБ» // Телекоммуникации. – 2019. – № 9. – С. 33-40.

Статья поступила в редакцию 6 июня 2020 г.
Принята к публикации 26 сентября 2020 г.

Ссылка для цитирования: Буйневич М.В., Израилов К.Е., Покусов В.В., Ярошенко А.Ю. Основные принципы проектирования архитектуры современных систем защиты // Национальная безопасность и стратегическое планирование. 2020. № 3(31). С. 51-58. DOI: https://doi.org/10.37468/2307-1400-2020-3-51-58