СИСТЕМАТИЗАЦИЯ ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ И ПАТЕНТНЫХ РАЗРАБОТОК В ОБЛАСТИ НЕФТЕГАЗОВОГО ОБОРУДОВАНИЯ

Ларионов К.О.
Email: Larionov17163@scientifictext.ru

Ларионов Константин Олегович – аспирант,
кафедра вычислительной техники и защиты информации,
Оренбургский государственный университет, г. Оренбург

Аннотация: *в статье анализируется предметная область состояния нефтегазового оборудования. Актуальность разработки и внедрения методов защиты информационного и программного обеспечения систем управления объектами нефтегазодобычи на основе прогнозирования моделей угроз обуславливается большим объемом затрат на обеспечение информационной безопасности. Актуальность выбранного направления исследований определена широким спектром применяемых методов защиты информационного и программного обеспечения. Определен уровень современных научных исследований предметной области и аналогичных патентных разработок.*
Ключевые слова: *защита, система, информация, программное обеспечение, нефтегазовое оборудование, анализ, методы защиты.*

SYSTEMATIZATION OF LITERARY SOURCES AND PATENT DEVELOPMENTS IN THE FIELD OF OIL AND GAS EQUIPMENT

Larionov K.O.

Larionov Konstantin Olegovich – Postgraduate,
DEPARTMENT OF COMPUTING AND INFORMATION SECURITY,
ORENBURG STATE UNIVERSITY, ORENBURG

Abstract: *the article analyzes the subject area of the state of oil and gas equipment. The relevance of the development and implementation of methods for protecting information and software systems for managing oil and gas production facilities based on predicting threat models is due to the large volume of costs for ensuring information security. The relevance of the chosen direction of research is determined by a wide range of applied methods of protecting information and software. The level of modern scientific research of the subject area and similar patent developments has been determined.*
Keywords: *protection, system, information, software, oil and gas equipment, analysis, protection methods.*

УДК 005

В числе отраслей-лидеров, выделяющих наибольшую долю ИТ-бюджета на информационную безопасность, в 2019 году можно отметить государственный и финансовый секторы, промышленность и топливноэнергетический комплекс (ТЭК) [36].

На рисунке 1 представлены статистические данные затрат на обеспечение информационной безопасности по сферам деятельности.

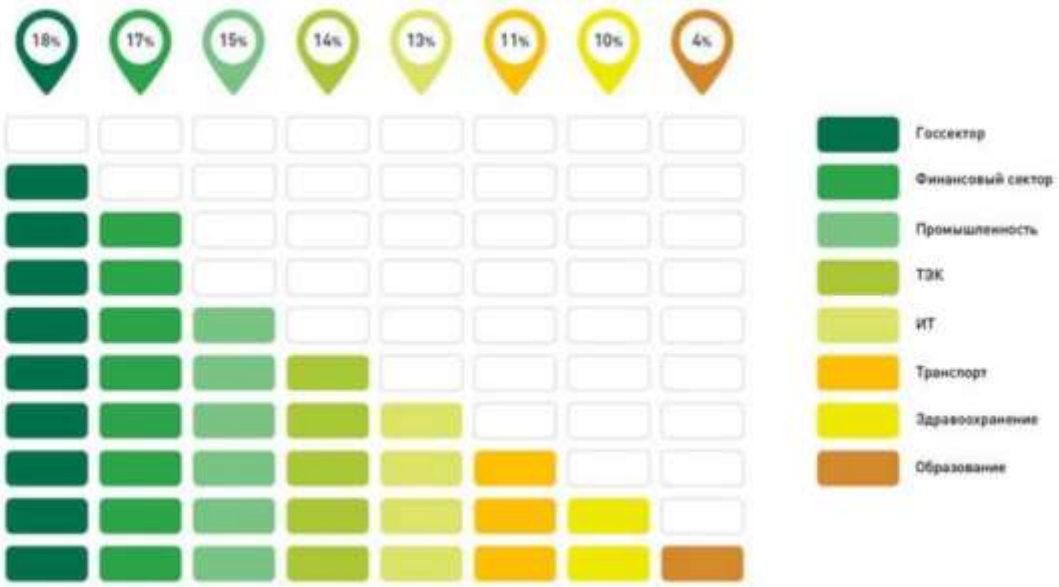

Рис. 1. Среднеотраслевое значение затрат на обеспечение информационной безопасности

В сфере ТЭК на обеспечение информационной безопасности выделяется 15% общего IT-бюджета. Это объясняется наличием в этом сегменте большого количества значимых информационных систем, требующих особой защиты.

Вопрос выбора средств защиты информации занимает отдельное место в теории обеспечения защиты информации, так как перед специалистом стоит множество задач, начиная с анализа рынка существующих решений, заканчивая обоснованием необходимости выбранного средства. Для того, чтобы определить наиболее подходящее средство защиты необходимо иметь определенные знания и обладать компетенцией в решении данной задачи. Так же необходимо четко поставить цель и требования к потенциальному продукту защиты информации и изучить методологии его внедрения.

Так, например, на рисунке 2 представлены критерии выбора средств защиты информации за 2019 год в сравнении с 2018 годом.

Рис. 2. Критерии выбора средств защиты информации

Всё в большей степени заказчикам требуется реальная безопасность, которую можно обеспечить просто, легко и надежно и которая соответствует текущим бизнес-задачам. При этом даже ценовой фактор перестает быть определяющим. Приоритетными критериями выбора средств защиты данных стали производительность, простота развертывания и качество продукта. Клиентоориентированность,

лидерство поставщика отодвинулись на второй план.

Целью исследования является систематизация информации в сфере разработки и внедрения методов защиты информационного и программного обеспечения систем управления объектами нефтегазодобычи на основе прогнозирования моделей угроз.

Для достижения цели поставлены следующие задачи:

1 Сбор и обработка информации в предметной области

Для определения концепции исследования необходимо провести аналитический обзор современных публикаций на тему разработки методов защиты информационного и программного обеспечения распределенных систем управления объектами нефтегазодобычи на основе прогнозирования моделей угроз.

Аналитический обзор современных научных работ позволяет разделить публикации по содержанию на следующие группы:

- публикации, отражающие современный уровень исследуемой области;
- публикации и патентные разработки, являющиеся аналогами разрабатываемой системе;
- публикации, определяющие используемые методы и средства для разработки;
- публикации, определяющие дальнейшие перспективы разработки;
- публикации, посвященные решению частных задач защиты информационного и программного обеспечения.

К первой группе публикаций относятся работы, посвященные анализу состояния нефтегазового оборудования. В частности, к данной теме можно отнести работы Крапивиной И.Е., Петрыкиной Т.Н., Тетеревлёвой Е.В. [17], Завьялова А.П. [11].

Анализ работ, отнесенных к первой группе, позволил определить особенности автоматизированных систем нефтегазодобычи и уровень развития методов и средств защиты информационного и программного обеспечения.

Ко второй группе публикаций относятся научные исследования и зарегистрированные программные и программно-аппаратные продукты, которые являются аналогичными разрабатываемой системе защиты информационного и программного обеспечения распределенных систем управления объектами нефтегазодобычи на основе прогнозирования моделей угроз. Данная тема исследований отражена в работах [1, 4], в диссертационных исследованиях [10, 23, 30] и в ряде патентных разработок [24-27].

Анализ публикаций, отнесенных ко второй группе, позволил определить дальнейшее направление исследований и предполагаемую научную новизну разрабатываемой системы.

К третьей группе отнесены публикации, определяющие методическую направленность исследований. Рассмотрены положения ГОСТов [7-8], руководящие документы ФСТЭК [2, 21], которые отражают основные рекомендации по защите информации в автоматизированных системах. Так же рассмотрен ряд публикаций по теории применения методов и средств защиты информационного и программного обеспечения, управлению объектами нефтегазодобычи, анализу и прогнозированию временных рядов, оптимизации рабочих процессов и построению распределенных вычислительных систем [3, 6, 12-13, 16, 22, 28, 32].

К четвертой группе публикаций относятся работы, которые позволили определить дальнейшее направление исследований. В работах [5, 33] изложены современные принципы и подходы к обеспечению информационной безопасности автоматизированных систем управления технологическими процессами. Приведены примеры осуществления сложных атак на автоматизированные системы управления. Изложены основные положения нормативно-методической документации, учитывающей лучшие мировые и отечественные практики в области обеспечения информационной безопасности промышленных систем. Проведен анализ базовых наборов мер защиты информации автоматизированных систем управления технологическими процессами. Рассмотрены основные современные средства обеспечения доступности промышленных систем. Предложен новый подход и поставлена задача разработки системы анализа состояния технического объекта.

2 Выявление проблемы предметной области

Главным достоинством рассмотренных работ является то, что они описывают широкий диапазон методов защиты информационного и программного обеспечения распределенных систем управления объектами нефтегазодобычи.

Однако, в ряде задач было необходимо провести полное исследование методов защиты информации и разработать метод защиты информационного и программного обеспечения распределенных систем управления объектами нефтегазодобычи на основе прогнозирования моделей угроз.

Актуальность выбранного направления исследований определена широким спектром применяемых методов защиты информационного и программного обеспечения.

Таким образом, к пятой группе публикаций отнесены работы, посвященные разработке и исследованию методов защиты информационного и программного обеспечения распределенных систем.

Вопросу разработки методов защиты программного обеспечения посвящены работы Комякова Д.С. [14], Кубашевского Д.В., Чернышовой А.В. [18]. Разработка и исследование методов защиты веб-приложений описана в работах Михеевой О.И., Гатчина Ю.А., Савкова С.В., Хамматовой Р.М., Ныркова А.П. [20], Хорошенко С.В., Бороненко С.Д., Ильяшенко О.Ю., Койвунена А.В. [31]. Исследование частных моделей угроз информационной безопасности представлено в работах Гудова Г.Н., Купач О.С. [9], Чернова Д.В., Сырчугова А.А. [34]. Методы обеспечения защиты средств информационных и коммуникационных систем описаны в работах Кондратьева А.А., Талалаева А.А., Тищенко И.П., Фраленко В.П., Хачумова В.М. [15], Куринных Д.Ю., Сахно В.В. [19], Шихнабиевой Т.Ш., Ахмедова О.К., Лобанкова Д.В. [35]. Математические модели прогнозирования описываются в работах Сауренко Т.Н., Анисимова В.Г., Анисимова Е.Г., Горбатова М.Ю., Сонькина М.А., Грачева В.Л. [29].

Обзор и анализ существующих разработок показал, что в современных научных исследованиях все большее внимание уделяется защите информации. Также ведутся разработки новых методов и методологий защиты информации на производстве, однако, при организации распределенной информационной вычислительной системы необходимо учитывает её особенности и специфику предприятия, для которого ведутся разработки.

Список литературы / References

1. *Ажмухамедов И.М.* Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / Ажмухамедов И.М., Князева О.М. Астрахань: Издательство: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Астраханский государственный университет" (Астрахань), 2015. С. 24-39.
2. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007). [Электронный ресурс]. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya- model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v- informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god/ (дата обращения: 10.09.2020).
3. *Барабанов А.В.* О систематике информационной безопасности цепей поставки программного обеспечения / Барабанов А.В., Марков А.С., Цирлов В.Л. Москва: Издательство: КлАССное снаряжение (Москва, 2019. С. 68-79.
4. *Басыня Е.А.* Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Басыня Е.А.; Новосибирск: Издательство: КлАССное снаряжение (Москва), 2018. С. 42-51.
5. *Гарбук С.В.* Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты / Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Москва: Издательство: Закрытое акционерное общество «Научно-производственное объединение «Эшелон» (Москва), 2019. С. 63-71.
6. *Глущенко В.М.* Модель прогнозирования безопасности и стабильности на основе интеграции рисков от угроз / Глущенко В.М., Елизаров В.С., Лузянин В.П. Москва: Издательство: Межрегиональная общественная организация «Академии военных наук» (Москва), 2006. С. 76-84;
7. ГОСТ 24.701-86. Надёжность автоматизированных систем управления. Основные положения. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/gost-24-701-86/ (дата обращения 10.09.2020).
8. ГОСТ Р 51028-97. Устройство защиты от ошибок аппаратуры передачи данных. Методы защиты. Москва: Издательство стандартов, 1997. 38 с.
9. *Гудов Г.Н.* Разработка математической модели нарушителя при реализации угроз безопасности информации / Гудов Г.Н., Купач О.С. Москва: Издательство: Московский финансово-юридический университет МФЮА (Москва), 2014. С. 181-185.
10. *Жуковский Е.В.* Анализ безопасности киберфизических систем с использованием методов машинного обучения. Диссертация на соискание учёной степени кандидата наук / Е.В. Жуковский. Санкт-Петербург: ФГАОУ ВО СПбПУ, 2019. 152 с.
11. *Завьялов А.П.* Технико-экономический анализ мониторинга технического состояния технологического оборудования / Завьялов А.П. Москва: Издательство: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина (Москва), 2020. С. 83-87.
12. *Захарова И.Г.* Интеграция математической и компьютерной подготовки в магистерской программе "разработка, администрирование и защита вычислительных систем" / Захарова И.Г. Тюмень:

Издательство: Пермский государственный национальный исследовательский университет (Пермь), 2017. С. 42-46.
13. *Израилов К.Е.* Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети / Израилов К.Е.;Санкт-Петербург: Издательство: Санкт-Петербургский государственный экономический университет (Санкт-Петербург), 2012. С. 150-153.
14. *Комяков Д.С.* Обзор методов внедрения статических водяных знаков в исходный код программного обеспечения / Комяков Д.С., Елсаков С.М. Челябинск: Издательство: Издательский центр ЮУрГУ (Челябинск), 2015. С. 84-92.
15. *Кондратьев А.А.* Методологическое обеспечение интеллектуальных систем защиты от сетевых атак / Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. Переславль-Залесский: Издательство: Издательский Дом "Академия Естествознания" (Пенза), 2014.
16. *Котенко И.В.* Перспективные направления исследований в области компьютерной безопасности / Котенко И.В., Юсупов Р.М. Санкт-Петербург: Издательство: Издательский Дом "Афина" (Санкт-Петербург), 2006.- С. 46-57.
17. *Крапивина И.Е.* Эффективность внедрения автоматизированного коррозионного мониторинга реального времени и перспективы развития на нефтепромысловых объектах / Крапивина И.Е., *Петрыкина Т.Н., Тетеревлёва Е.В.* Ухта: Издательство: Ухтинский государственный технический университет (Ухта), 2013. С. 77-80.
18. *Кубашевский Д.В.* Исследование методов и средств защиты авторского права в области разработки программного обеспечения для распределённых систем / Кубашевский, Д.В., Чернышова А.В. Донецк: Издательство: Донецкий национальный технический университет (Донецк), 2018. С. 109-115.
19. *Куринных Д.Ю.* Методы обеспечения защиты средств информационных и коммуникационных систем / Куринных Д.Ю., Сахно В.В. Ростов-на-Дону: Издательство: Индивидуальный предприниматель Кузьмин Сергей Владимирович (Казань), 2019. С. 44-46.
20. *Михеева О.И.* Методы поиска аномальных активностей веб-приложений / Михеева О.И., Гатчин Ю.А., Савков С.В., Хамматова Р.М., Ныркова А.П. Санкт-Петербург: Издательство: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Санкт-Петербург), 2020. С. 233-242.
21. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ от 11 февраля 2013 г. № 17. М., 2013.
22. *Панкратов С.А.* Разработка и внедрение комплекса методов автоматизации бизнес-процессов и защиты корпоративного программного и информационного обеспечения производственно-заготовительного предприятия по переработке текстильного вторсырья / Панкратов С.А. Диссертация кандидата технических наук. Московский государственный университет дизайна и технологии. Москва, 2013.
23. *Паньков А.Н.* Разработка, исследование и совершенствование методов испытаний программного обеспечения средств измерений. Диссертация на соискание учёной степени кандидата наук / Паньков А.Н. Москва. Всероссийский научно-исследовательский институт метрологической службы Российской Федерации, 2016. 170 с.
24. Патент 2693683, Российская Федерация, МПК H04L 12/26, G06F 11/00. Автоматизированная система контроля информационной устойчивости полевого узла связи / Уланов А.В., Вергелис Н.И.; заявитель и патентообладатель: Федеральное государственное бюджетное учреждение "16 Центральный научно-исследовательский испытательный ордена Красной Звезды институт имени маршала войск связи А.И. Белова" Министерства обороны Российской Федерации; заявл. 16.05.2018; опубл. 03.07.2019 Бюл. № 19.
25. Патент 2701994 Российская Федерация, МПК G06F 1/00. Способ моделирования виртуальных сетей в условиях деструктивных программных воздействий / Алисевич Е.А., Бречко А.А., Львова Н.В., Сорокин М.А., Стародубцев Ю.И.; заявитель и патентообладатель: Алисевич Е.А., Бречко А.А., Львова Н.В., Сорокин М.А., Стародубцев Ю.И.; заявл. 15.10.2018; опубл. 02.10.2019, Бюл. № 28.
26. Патент 2704268 Российская Федерация, МПК H04L 9/08, H04W 12/06. Способ, система и устройство криптографической защиты каналов связи беспилотных авиационных комплексов / Борисов К.В., Любушкина И.Е., Панасенко С.П., Романец Ю.В., Сиротин А.В., Сырчин В.К.; заявитель и патентообладатель: Общество с ограниченной ответственностью Фирма "АНКАД"; завял. 18.05.2018; опубл. 25.10.2019 Бюл. № 30.
27. Патент 2706176, Российская Федерация, МПК G06F 21/60. Способ обеспечения криптографической защиты информации в сетевой информационной системе / Ерыгин А.В.; заявитель и патентообладатель: Открытое акционерное общество "Информационные технологии и коммуникационные системы"; заявл. 31.05.2019; опубл. 14.11.2019 Бюл. № 32.

28. *Рудниченко А.К.* Защита от вредоносного программного обеспечения, представляющего собой комплекс легитимных программных продуктов / Рудниченко А.К., Колесникова Д.С., Верещагина Е.А. Владивосток: Издательство: Издательский центр "Науковедение" (Москва), 2017.
29. *Сауренко Т.Н.,* Математические модели прогнозирования экологической угрозы техногенных аварий и катастроф в составе интегрированных систем безопасности региона / Сауренко Т.Н., Анисимов В.Г., Анисимов Е.Г., Горбатов М.Ю., Сонькин М.А., Грачев В.Л. Москва: Издательство:Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России (Москва), 2019. С. 62-67.
30. *Сизоненко А.Б.* Модели и алгоритмы синтеза логико-вычислительных подсистем защиты информации систем критического применения. Диссертация на соискание учёной степени доктора наук / Сизоненко А.Б. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2016. 310 с.
31. *Хорошенко С.В.* Угрозы безопасности SQL-инъекций для WEB-приложений / Хорошенко С.В., Бороненко С.Д., Ильяшенко О.Ю., Койвунен А.В. Санкт-Петербург: Издательство: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (Санкт-Петербург), 2013. С. 654-659.
32. *Чакрян В.Р.* Информационная безопасность в Российской Федерации / Чакрян В.Р., Дубровская Т.А. Сочи: Издательство: Общество с ограниченной ответственностью "Профпресс" (Ростов-на-Дону), 2019. С. 317-321.
33. *Чернов Д.В.* Современные подходы к обеспечению информационной безопасности АСУ ТП / Чернов Д.В., Сычугов А.А. Тула: Издательство: Тульский государственный университет (Тула), 2018. С. 58-64.
34. *Чернов Д.В.* Формализованное представление модели угроз информационной безопасности АСУ ТП / Чернов Д.В., Сычугов А.А. Тула: Издательство: Издательство "Радиотехника" (Москва), 2019. С. 74-80.
35. *Шихнабиева Т.Ш.* Совершенствование системы обеспечения информационной безопасности компании на основе использования интеллектуальных методов и моделей / Шихнабиева Т.Ш., Ахмедов О.К., Лобанков Д.В. Москва: Издательство: Общество с ограниченной ответственностью "Научный консультант" (Москва), 2017. С. 484-489.
36. «Код безопасности» определил ключевые факторы расходов на ИБ в 2019 г. [Электронный ресурс]. Режим доступа: https://www.itweek.ru/security/news- company/detail.php?ID=206250/ (дата обращения 10.09.2020).