**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ПРОГРАММИРОВАНИЯ

ЦИФРОВЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

Сборник научных статей

Под редакцией Е.В. Стельмашонок, И.Н. Васильевой

**ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО
ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2020**

ББК 32.971.35-5
Ц75

Ц75 **Цифровые** технологии обработки и защиты информации : сборник научных статей / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2020. – 161 с.

ISBN 978-5-7310-4807-1

В сборнике научных статей рассмотрены проблемы информационной безопасности, сопровождающие процессы цифровизации экономики и других областей человеческой жизни, модели, методы и средства защиты информации в компьютерных системах и связанные организационно-правовые вопросы.

Сборник будет полезен преподавателям и обучающимся по направлениям, связанным с информационными технологиями и информационной безопасностью, а также всем, кто интересуется проблемами развития современных цифровых технологий.

The scientific papers examines the information security problems accompanying the processes of digitalization of the economy and other areas of human life, models, methods and means of information security in computer systems and related organizational and legal issues.

The publication can be useful to teachers and students studying in information technologies and information security, as well as to everyone who is interested in the problems of the development of modern digital technologies.

ББК 32.971.35-5

Рецензенты:
профессор СПб университета МВД России, заслуженный деятель науки РФ, д-р техн. наук, проф. **В.И. Куватов**
зав. кафедрой информатики СПбГЭУ заслуженный деятель науки РФ, д-р техн. наук, проф. **В.В. Трофимов**

ISBN 978-5-7310-4807-1

© СПбГЭУ, 2020

СОДЕРЖАНИЕ

Андреевский И.Л. Вопросы обеспечения информационной безопасности облачных программных продуктов 5

Баулина А.С., Полубарова И.В. Применение метода анализа иерархий для оценки актуальности угроз при составлении частной модели угроз безопасности информационных систем персональных данных университета 9

Бесклубов С.В., Мотиков М.О. Исследование аппаратной технологии удаленного администрирования iKVM, предназначенной для автономного мониторинга и удаленного управления серверных платформ ASUS 15

Бурзунов Д.Д., Крайковский Г.А. Разработка концепции системы автоматического анализа сетевого трафика на основе моделей самообучения и использования статистических методов классификации данных 26

Васильева И.Н. Обеспечение целостности системных ресурсов в операционных системах Windows и Linux 29

Васильева И.Н., Чернокнижный Г.М. Правовые основания использования средств мониторинга в корпоративной информационной среде 48

Верзилова А.С. Использование деловых игр при обучении бакалавров информационной безопасности 54

Гниденко И.Г., Егорова И.В. Критерии выбора DLP-систем 59

Горшков А.А., Федоров Д.Ю., Астахов А.Ю., Зиангиров О.А., Зимин В.А. Обоснование критериев перевода системы обучения инженерных кадров в автоматизированную среду подготовки 65

Зарипов Б.И., Лямзин О.С. Состояние и перспективы развития производителей коммутационного оборудования Cisco и D-Link 71

Ильина Д.А., Солодянников А.В. Особенности руководства по качеству подразделения по защите информации предприятия малого бизнеса 75

Кухарь В.В., Никифоров А.А. Вопросы правового регулирования безопасности Интернета вещей 78

Майорова Е.В., Соколовская С.А., Черток А.В. Обеспечение информационной безопасности при гибком подходе разработки программного продукта 83

Морозов С.К., Красильникова Е.В. Информационная безопасность систем управления современного автотранспорта с точки зрения потенциальной возможности реализации внешних угроз 93

Петров В.Г. Алгоритм (этапы) создания системы обработки и обеспечения безопасности персональных данных в организации 96

Полегенько А.М. О проблемах развития концепции Интернета вещей 103

Синещук Ю.И. Метод оценки эффективности организации безопасного информационного взаимодействия элементов распределенной вычислительной сети 108

Солодянников А.В. Особенности сбора информации о кандидате на должность сотрудника подразделения защиты информации на предприятии 116

Стельмашонок Е.В., Стельмашонок В.Л. Организация инфраструктуры системы защиты информации в составе информационной инфраструктуры предприятия 129

Сухостат В.В. Особенности разработки методов и моделирования информационной защищенности оператора автоматизированных систем 135

Якубов М.С., Кулдашев Л.С. Алгоритм выбора рациональной функциональной структуры многостадийных процессов 152

УДК 004.056

Вопросы обеспечения информационной безопасности облачных программных продуктов

И. Л. Андреевский, к.э.н., доцент,
Санкт-Петербургский Государственный Экономический Университет

Облачные технологии появились сравнительно недавно, обрели свою популярность, достигли технологической зрелости. Данный сегмент рынка активно развивается. В условиях развития цифровой экономики облачные технологии стали одной из ключевых инфраструктурных технологий.

Среднестатистический облачный программный продукт является распределенным приложением, в котором есть клиентская часть, слой бизнес-логики, слой доступа к данным, хранилище данных (база данных). База данных, компоненты слоя доступа к данным и бизнес-логики требуют места в облачном хранилище. Использование облачных технологий требует специализированной ИТ-инфраструктуры, развертывания центра обработки данных (ЦОД).

На практике такая архитектура построения облачного приложения с учетом требований по надежности, отказоустойчивости, высокой доступности, информационной безопасности и др. добавляет целых ряд своих дополнительных специализированных облачных компонентов или сервисов, использование которых также влияет на конечную стоимость продукта.

На текущий момент получили распространение следующие облачные модели обслуживания [1]:

– программное обеспечение как сервис (Software as a Service, SaaS), которая предполагает, что потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре;

– платформа как сервис (Platform as a Service, PaaS), в которой контроль и управление основной физической и виртуальной инфраструктурой облака осуществляется облачным провайдером, за исключением разработанных или установленных приложений, а также, по возможности, параметров конфигурации среды (платформы);

– инфраструктура как сервис (Infrastructure as a Service, IaaS). В модели обслуживания IaaS потребитель может контролировать операционные системы, виртуальные системы хранения данных и установленные приложения, а также ограниченный контроль набора доступных сервисов. Контроль и управление основной физической и виртуальной инфраструктурой облака осуществляется облачным провайдером.

Кроме этого, принято выделять следующие модели развертывания «облачных сред» на базе ЦОД:

– частное (закрытое) облако (private cloud),
– публичное (открытое) облако (public cloud),
– общественное облако (community cloud),
– смешанное (или гибридное) облако (hybrid cloud).

Каждая из моделей обслуживания и развертывания имеет свои особенности, которые подробно рассматриваются на различных информационных ресурсах в том числе в сети Интернет.

Вне зависимости от используемой модели обслуживания, развертывания конечный потребитель облачных программных продуктов за потраченные финансовые ресурсы хочет получить готовое решение, достаточно часто забывая о вопросах информационной безопасности. В основе такого подхода чаще всего лежит ассоциация облачных технологий с услугами по аутсорсингу обработки и хранения данных пользователя, при котором взимаемая плата гарантирует качественное выполнение данных услуг. Однако ответственность за безопасность облачных данных, сетевой инфраструктуры, т.д. на практике оказывается распределена между несколькими участниками, и граница зон ответственности чаще всего четко не прописана.

Развертывание в облаке требует от всех участников взаимодействия (пользователей облачных программных продуктов, предприятий информатизации по производству облачных программных продуктов, предприятий информатизации по проектированию облачных информационных систем, предприятий информатизации по обработке облачных данных (центры обработки данных, ЦОД)) определенных усилий в области информационной безопасности, минимизации «поверхности атаки».

Появилось целое направление информационной безопасности в облаке – это «безопасность как услуга» или Security as a Service (SECaaS).

Зоны ответственности со стороны предприятия информатизации при разработке облачного программного продукта представлены ниже (таблица 1, составлено по материалам источника [3]).

Анализ различных литературных источников, онлайн ресурсов в сети Интернет, посвященных облачной информационной безопасности показал, что комплексный взгляд на данную проблему для всех участников облачной информатизации представлен недостаточно полно.

Предлагаются различные модели облачной безопасности, например, работы [5; 6], ориентированные на технический аспект ее обеспечения.

В работе [6] предлагается подход к оценке уровня зрелости политики информационной безопасности, конфиденциальности и соответствия с уровнями зрелости модели Capability Maturity Model (CMM).

Таблица 1 – Уровень контроля со стороны предприятия информатизации по разработке облачного программного продукта при разных моделях обслуживания облачного программного продукта

Компоненты ИТ инфраструктуры / Уровень контроля	Разработчика		
	PaaS	IaaS	Собственная инфраструктура (частное облако)
Сетевая инфраструктура			+
Хранилище данных			+
Платформа виртуализации			+
Аппаратная платформа			+
Серверы			+
Базы данных		+	+
Безопасность и интеграция		+	+
Среда выполнения		+	+
Приложения	+	+	+

В источнике [8] предлагается создание платформы по безопасности, включающей: пользовательский уровень, уровень для проведения облачного аудита; уровень авторизации и аутентификации, уровень управления уровнем доступа, уровень данных, уровень виртуализации, физический уровень.

Для каждого уровня предполагается ряд мероприятий, преимущественно технической направленности в области обеспечения необходимого уровня информационной безопасности.

В различных работах перечисляются отдельные факторы и аспекты информационной безопасности, например, источники [4; 7].

В тоже время необходимо комплексное рассмотрение вопросов информационной безопасности в сфере разработки и эксплуатации облачных программных продуктов с учетом всех участников облачного взаимодействия (рисунок 1).

Вопросы обеспечения информационной безопасности облачных программных продуктов должны рассматриваться в нескольких аспектах – юридическом, организационном и техническом [2]. Должна быть принята и действовать стратегия по обеспечению информационной безопасности при работе с облачными программными продуктами.

Целесообразно переходить к проактивному управлению информационной безопасностью. Сиюминутная экономия на вопросах облачной информационной безопасности может в дальнейшем обернуться значительными убытками.

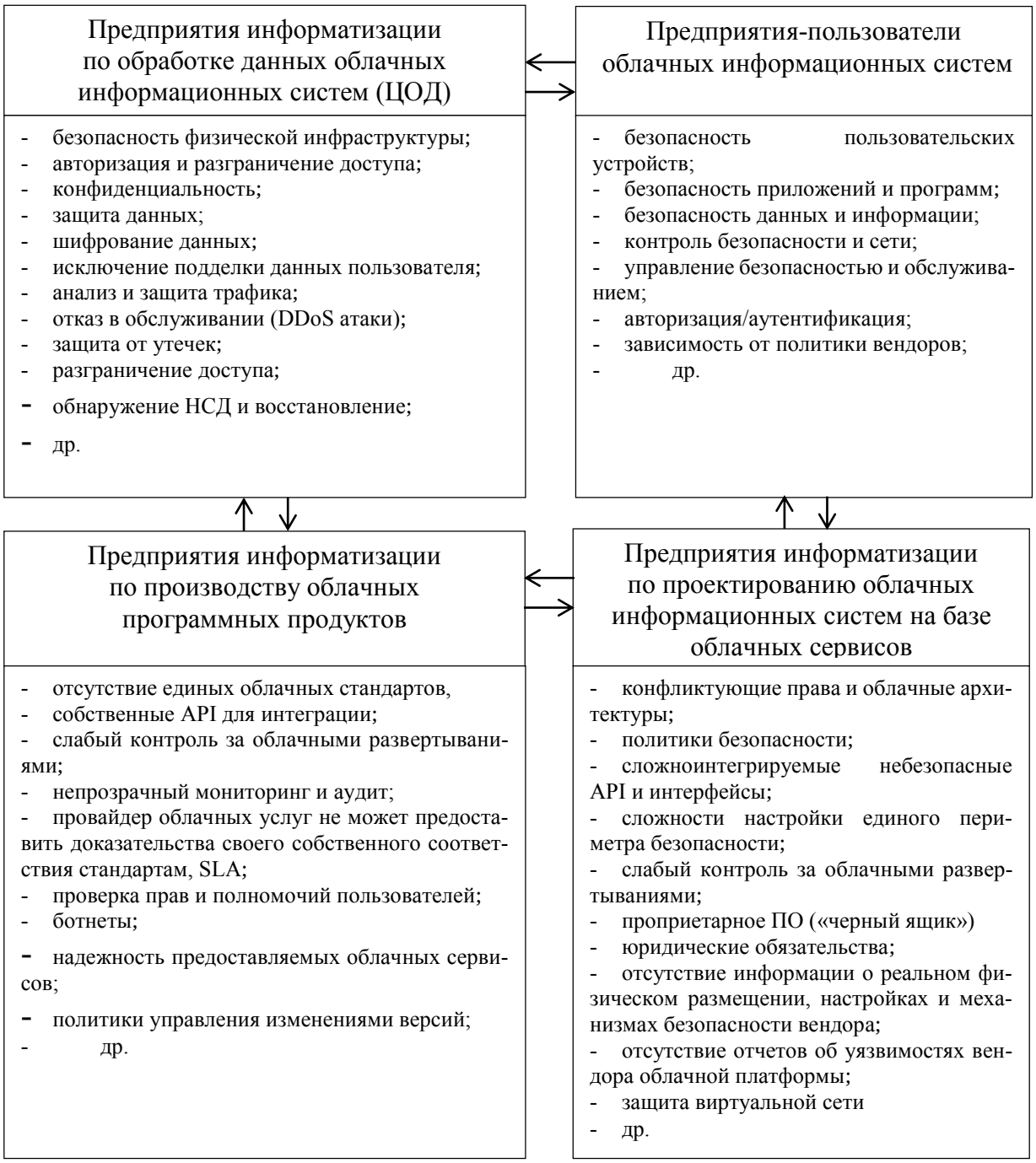

Рисунок 1 – Вопросы информационной безопасности в сфере разработки и эксплуатации облачных программных продуктов

Список литературы

1. Андреевский И. Л. Разработка бизнес-приложений с использованием облачной инфраструктуры: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016.–59с.
2. Андреевский И. Л. Технологии облачных вычислений: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2018. – 80 с.

3. Информационный портал по платформе облачных вычислений Microsoft Azure. [Электронный ресурс] - Режим доступа: https://azure.microsoft.com/ru-ru
4. Abdelrafe Elzamly, Burairah Hussin, Abd Samad Hasan Basari Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study // International Journal of Grid and Distributed Computing Vol. 9, No. 8, (2016), pp.137-158
5. Abdelrafe Elzamly, Burairah Hussin, Samy Abu Naser, Khalid Khanfar, Mohamed Doheir, and Ali Selamat, Abdullah Rashed A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations // International Journal of Grid and Distributed Computing Vol. 9, No. 9 (2016), pp.137-154
6. Fahad F. Alruwailia, T. Aaron Gulliver Secure migration to compliant cloud services: A case study // Journal of Information Security and Applications. Vol 38, Feb. 2018, pp. 50-64.
7. Gozmana D., Willcocksc L. The emerging Cloud Dilemma: Balancing innovation with cross-border // Journal of Business Research 97 (2019) pp. 235–256.
8. Hui, H, McLernon, D and Zaidi, A Design of the Security Mechanism for a BPO Cloud Computing Platform. In: Proceedings of the ICSESS 2018: IEEE 9th International Conference on Software Engineering and Service Science, 23 Nov - 25 Aug 2018, Beijing, China. IEEE , pp. 1092-1095.

УДК 004.056

Применение метода анализа иерархий для оценки актуальности угроз при составлении частной модели угроз безопасности информационных систем персональных данных университета

А. С. Баулина, магистрант
И. В. Полубарова, магистрант
Санкт-Петербургский Государственный Экономический Университет

В статье описывается возможность применения метода анализа иерархий при оценке угроз безопасности персональных данных. Данный метод ранжирует степень важности каждой угрозы для компании в целом.

В университете обрабатывается большое количество персональных данных: персональные данные абитуриентов, студентов, сотрудников структурных подразделений и профессорско-преподавательского состава.

Защита обрабатываемых персональных данных является важной задачей для каждой организации. Нарушение конфиденциальности, целостности и доступности этой информации влечет за собой различной степени ущерб организации как финансовый, так и репутационный.

Для того, чтобы свести к минимуму потери и убытки от реализации угроз информационной безопасности необходимо ответственно подходить

к организации системы защиты информации, используя комплекс технических, программных и организационных мер по защите информации. Одной из организационных мер является составление модели угроз и модели нарушителя. Данные документы позволяют выявить актуальные угрозы безопасности данных, что помогает в большей степени спрогнозировать затраты на построение комплексной системы защиты информации организации. Это требует разработки такой политики безопасности, основанной на анализе информационных угроз, чтобы в рамках выделенного бюджета были обеспечены конфиденциальность, целостность и доступность информационных ресурсов организации [4].

В качестве данных для составления частной модели угроз (ЧМУ) могут послужить результаты аудита информационной безопасности, опроса сотрудников и зарегистрированных пользователей системы посредством анкетирования, методические и руководящие документы ФСТЭК и ФСБ России, в частности «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ЧМУ содержит сведения обо всех возможных угрозах, возможностях их реализации, актуальности их для системы и порядках их предотвращения для обеспечения стабильной работы информационной системы.

Со стороны Российского законодательства, работу с персональными данными регулирует 152-ФЗ «О персональных данных». Согласно 152-ФЗ, обеспечение безопасности персональных данных является обязанностью самого оператора персональных данных. Также существует ряд нормативно правовых актов, связанных с защитой персональных данных, которые направлены на защиту конституционных прав граждан, на неприкосновенность частной жизни, личную и семейную тайну, закрепленные в ст. 23 Конституции РФ.

Недостаточные меры по защите ПДн в организации могут привести к нарушению законных прав субъектов ПДн, повлечь за собой череду жалоб со стороны граждан в государственные органы, чьи права могут оказаться нарушенными в связи с разглашением конфиденциальной информации, и даже привлечению оператора ПДн к административной или уголовной ответственности.

В настоящее время существует огромное количество угроз персональных данных. Выбор наиболее актуальных из них может производиться на основе анализа источников угроз и их влияния на конкретную организацию. В статье применяется метод анализа иерархий для оценки важности угроз при составлении частной модели угроз безопасности информационных систем персональных данных университета.

Метод анализа иерархий – это математический подход, использующийся для принятия решений. Метод анализа иерархий был разработан американским математиком Томасом Л. Саати в 1970 году, после чего получил широкое распространение и до сих пор активно используется в управленческой деятельности. Этот метод не предоставляет анализирующему лицу верное решение, но позволяет самостоятельно найти наиболее предпочтительную альтернативу, согласующуюся с его пониманием сути проблемы, а также проследить влияние важности критериев на выбор альтернативы [1].

В ходе проведения исследования было использовано программное приложение для поддержки принятия решений SuperDecisions v 2.2, с помощью которого можно реализовать метод анализа иерархий (Analytic Hierarchy Process, AHP) и метод аналитических сетей (Analytic Net Process, ANP).

Для применения данного метода необходимо построение иерархической структуры, включающей в себя поставленную цель, наиболее важные критерии выбора и доступные альтернативы (рисунок 1). Целью исследования является выбор наиболее актуальных угроз безопасности для системы.

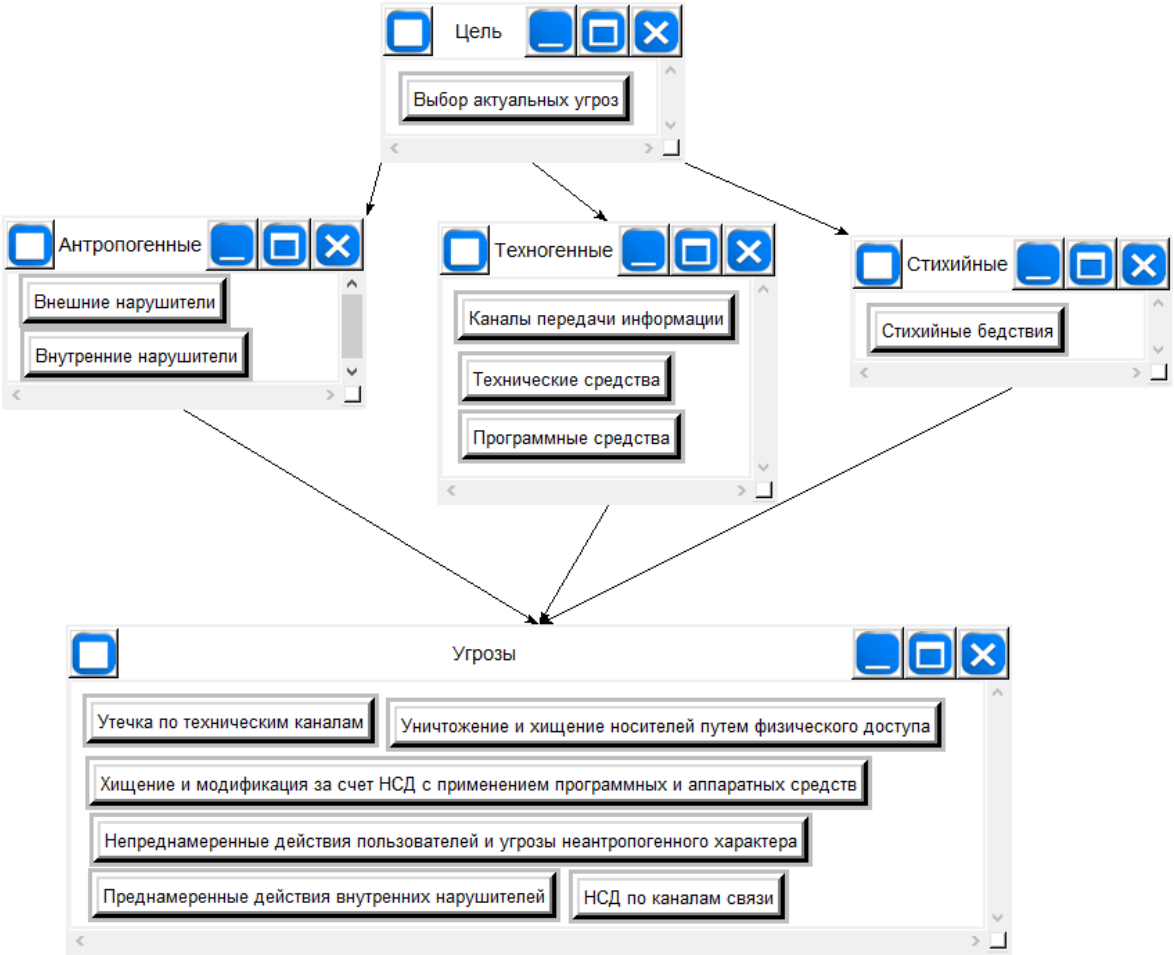

Рисунок 1 – Иерархическая структура модели выбора актуальных угроз

Следующий этап – определение приоритетов с помощью метода экспертной оценки методом парных сравнений. Значение «1» в матрице парных сравнений означает то, что критерии одинаково важны, «3» – умеренное превосходство, «5» – существенное превосходство, «7» – значительное превосходство, «9» – очень сильное превосходство. Числовые метки «2», «4», «6» и «8» обозначают соответствующие промежуточные значения.

Для проверки правильности экспертной оценки вводится индекс согласованности матрицы:

$$\text{ИС} = \frac{\lambda_{max} - n}{n-1},$$

где λ_{max} – максимальное собственное значение,

n – размерность матрицы.

Значение индекса согласованности более 0,1 свидетельствует о том, что мнения экспертов неправильны и следует перепроверить их суждения. В некоторых случаях ИС допустим до 0,2.

В результате экспертной оценки строится матрица парных сравнений для каждого из кластеров, визуально показывающая количественную предпочтительность одного элемента матрицы над другим. Для оценки важности угроз безопасности университета было построено 8 матриц, одна из которых представлена на рисунке 2.

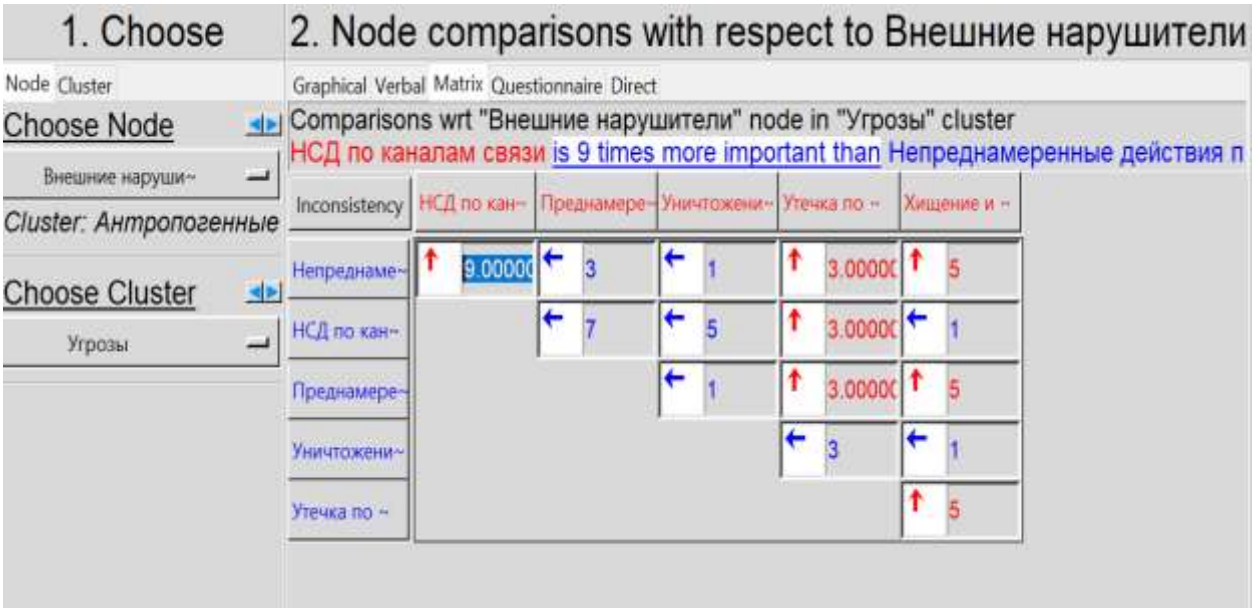

Рисунок 2 – Матрица попарных сравнений

В данной матрице показано, какие угрозы являются приоритетными для внешних нарушителей безопасности. Какие именно нарушители актуальны для определенной организации показывает модель нарушителя

безопасности. Модель нарушителя – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа [2].

На рисунке 3 представлен полученный вектор приоритетов. В нормализованном векторе приоритетов представлены 4 подгруппы приоритетов по количеству кластеров в иерархии. К ним относятся: антропогенные, техногенные и стихийные источники угроз, а также сами угрозы безопасности персональных данных. Проанализировав каждую подгруппу, можно сделать выводы о том, что для нашей системы наиболее актуальны внутренние нарушители безопасности, что логично, ведь территория университета является охраняемой зоной и нахождение посторонних лиц сведена к минимуму, также информация, обрабатываемая в системах университета, не является актуальной для внешних нарушителей серьезного уровня.

Here are the priorities.

Icon	Name	Normalized by Cluster	Limiting
No Icon	Внешние нарушители	0.12500	0.020833
No Icon	Внутренние нарушители	0.87500	0.145833
No Icon	Стихийные бедствия	1.00000	0.166667
No Icon	Каналы передачи информации	0.10615	0.017691
No Icon	Программные средства	0.70097	0.116829
No Icon	Технические средства	0.19288	0.032147
No Icon	Непреднамеренные действия пользователей и угрозы н~	0.23215	0.116073
No Icon	НСД по каналам связи	0.09887	0.049434
No Icon	Преднамеренные действия внутренних нарушителей	0.14493	0.072466
No Icon	Уничтожение и хищение носителей путем физическ~	0.21761	0.108804
No Icon	Утечка по техническим каналам	0.13056	0.065280
No Icon	Хищение и модификация за счет НСД с применением п~	0.17588	0.087942
No Icon	Выбор актуальных угроз	0.00000	0.000000

Рисунок 3 – Вектор приоритетов

Среди техногенных источников угроз преобладают программные средства. Среди самих угроз безопасности персональных данных выде-

ляются следующие наиболее актуальные угрозы (угрозы отсортированы по приоритету):

– непреднамеренные действия пользователей и угрозы не антропогенного характера;

– уничтожение и хищение носителей путем физического доступа;

– хищение и модификация за счет несанкционированного доступа (НСД) с применением программных и аппаратных средств.

Угрозу можно назвать актуальной, если она может быть реализована в данной системе и представляет для нее какую-либо опасность в результате реализации.

Для минимизации приведенных выше актуальных угроз необходимо использовать комплекс организационно-технических мер по защите информации. Например, если наиболее актуальной угрозой в нашем случае являются непреднамеренные действия внутренних нарушителей, то необходимо проводить обучение персонала по работе с системой и по защите информации, создать такие документы, как парольная политика, руководство пользователя и руководство администратора системы.

Планирование и организация мероприятий по защите персональных данных должны проводиться для всех видов угроз, уделяя особое внимание перечню именно актуальных угроз для рассматриваемой информационной системы обработки персональных данных. Необходимо отметить, что для нормального функционирования ключевых бизнес-процессов организации и надежной работы аппаратно-программного комплекса необходимо создать и поддерживать эффективную систему защиты информации.

Список литературы

1. Гриненко Г.А., Кучеренко Ю.А., Попова М.М. Использование метода анализа иерархий для оценки информационных угроз безопасности личности // Экономика и социум. – 2018. – № 1 (44). – С. 249-256.
2. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ. [Электронный ресурс] – М.: Гостехкомиссия России, 1992. URL: https://fstec.ru/component/ attachments/download/298 (дата обращения: 13.11.2019).
3. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь. – 1993. – 278 с.
4. Стельмашонок Е.В., Стельмашонок В.Л. Методические аспекты моделирования системы защиты информации в организации // Петербургский экономический журнал. – 2019. – № 2. – С. 64-70.

УДК 004.71, 004.056

Исследование аппаратной технологии удаленного администрирования iKVM, предназначенной для автономного мониторинга и удаленного управления серверных платформ ASUS

С. В. Бесклубов, студент группы ИБ-1601,
М. О. Мотиков, студент группы ИБ-1601,
Санкт-Петербургский Государственный Экономический Университет

Реализацией удаленного управления и мониторинга компьютерных систем крупные производители оборудования вплотную занялись еще в конце прошлого века. При стремительном росте компьютеризации и возникновении распределенных сетей крупных предприятий и организаций потребовалась технология, которая бы позволяла централизовано управлять наиболее важными узлами без непосредственного локального доступа к компьютеру. В результате этого родился такой стандарт, как IPMI. В статье производится обзор ключевых особенностей данного стандарта и анализ реализации аппаратной платформы удаленного администрирования от компании ASUS, основанной на наборе интерфейсов IPMI.

Описание стандарта IPMI

Intelligent Platform Management Interface (IPMI) – набор спецификаций интерфейсов, предназначенных для разработки и эксплуатации автономных подсистем, предоставляющих возможности для управления и мониторинга серверов независимо для основного процессора, микропрограммного обеспечения (BIOS или UEFI) и операционной системы. IPMI определяет набор интерфейсов, используемых системным администратором для внеполосного (out-of-band) доступа к системе. Например, IPMI предоставляет возможность управлять сервером, который может быть отключен, или просто недоступен через основное сетевой соединение. Также существует возможность удаленно установить операционную систему: без IPMI установка операционной системы потребовала бы физического доступа к системе, вставки DVD или USB устройства с образом устанавливаемой ОС и полного прохождения процесса установки с использованием монитора и клавиатуры; используя же IPMI, администратор может удаленно примонтировать ISO образ, симулируя таким образом DVD, и выполнить установку [1].

Первая версия спецификации была представлена компанией Intel в сентябре 1998 года. На данный момент последняя версия поддерживаеся более, чем 200 компьютерными компаниями-разработчиками, такими как Cisco, Dell, Hewlett Packard Enterprise, Intel, NEC Corporation, SuperMicro и Tyan.

IPMI функционал может работать в любом из трех случаев:

– До того, как основная ОС запущена

– Когда сервер отключен

– После того, как работа основной ОС была прервана в результате критической ошибки

Системный администратор может использовать IPMI-совместимую подсистему для отслеживания состояния платформы (например, температурных датчиков, напряжения, вентиляторов и состояния питания), для просмотра системных журналов, включения, выключения и перезагрузки. Также стандарт предусматривает механизмы оповещения о состоянии системы или о возникновении какого-либо события посредством SNMP (Simple Network Management Protocol) протокола.

Помимо внеполосного доступа с использованием выделенного сетевого разъема RJ-45 и своего сетевого интерфейса, также существует возможность настройки совместного (side-band) сетевого доступа с использованием общего соединения. Такое соединение организуется посредством SMBus (System Management Bus) интерфейса между IPMI подсистемой и основным сетевым интерфейсом сервера. Преимущество такого решения заключается в меньшей стоимости конечной системы и сокращения числа используемых разъемов.

Основные компоненты IPMI

Общая схема с изображением IPMI компонентов представлена на рисунке 1. IPMI подсистема состоит из главного контроллера, называемого Baseboard Management Controller (BMC) и других контроллеров управления, которые взаимодействуют с BMC с помощью интерфейса Intelligent Platform Management Bus (IPMB) – дополненной реализации I2C.

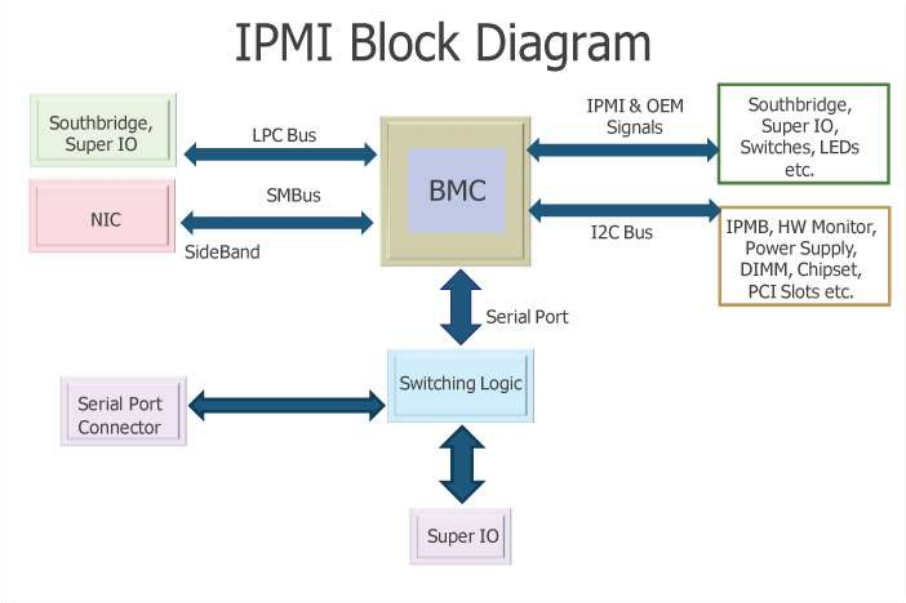

Рисунок 1 – Схема IPMI компонентов

Некоторые компании специально разрабатывают и продают BMC чипы. Они могут иметь ограниченную память и требовать оптимизированного встроенного ПО для реализации полной функциональности IPMI. Контроллеры BMC могут предоставлять сложные инструкции и полный внешний функционал.

Baseboard Management Controller является основным элементом IPMI-совместимой системы. Это специальный микроконтроллер, встроенный в материнскую плату сервера. BMC управляет интерфейсами между программным обеспечением для управления системой и оборудованием платформы.

Разные типы датчиков, встроенных в компьютерную систему, отправляют BMC такие параметры, как температура, скорость вращения вентиляторов, состояние питания и основной операционной системы. BMC принимает все показания датчиков, и затем может отправить эти данные системному администратору через сеть.

Описание интерфейсов

Диаграмма со *схематичным* изображением IPMI-интерфейсов приведена на рисунке 2.

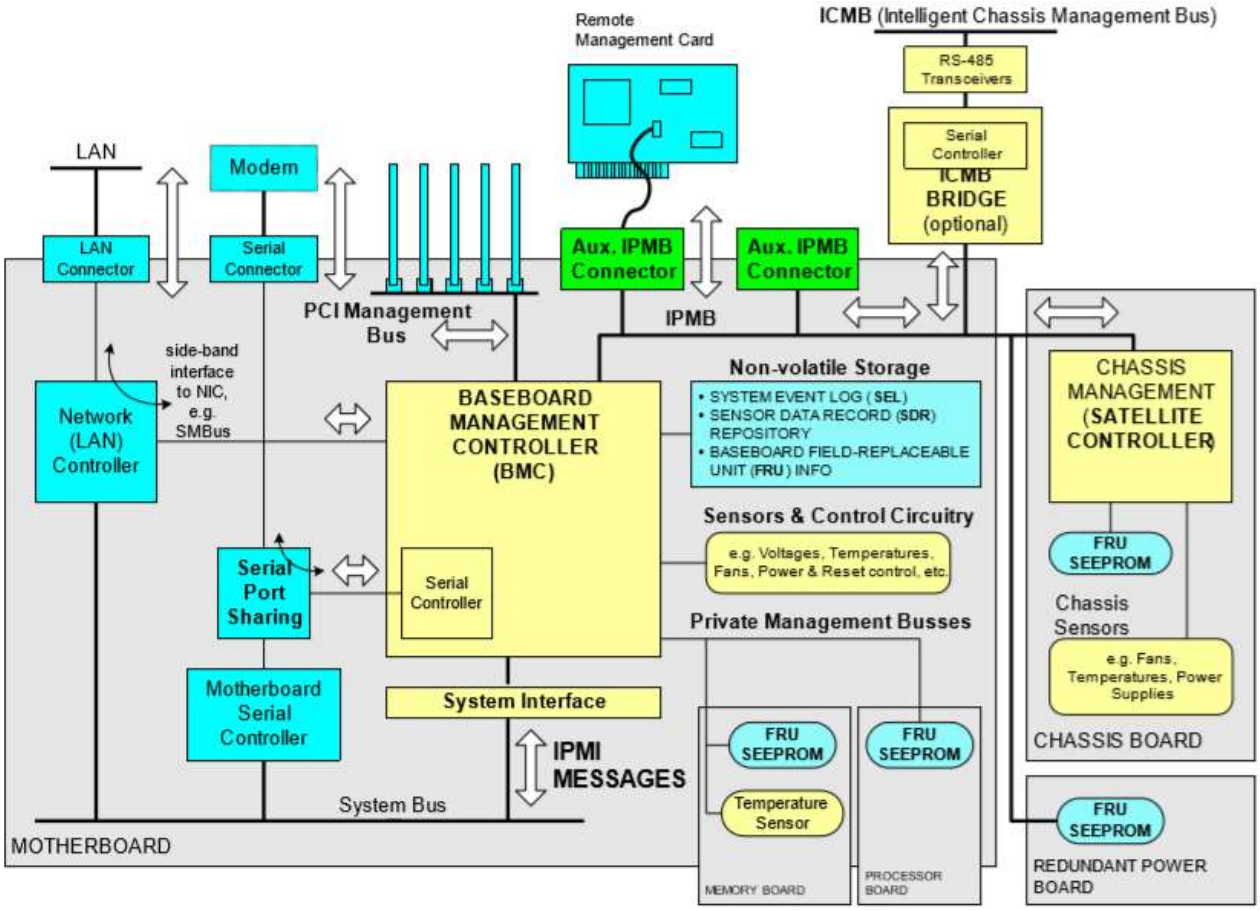

Рисунок 2 – Схема IPMI-интерфейсов

В IPMI используются интерфейсы, базирующиеся на протоколах обмена сообщениями. Все IPMI сообщения имеют общее поле, несущее полезную нагрузку (payload) независимо от того, какой используется интерфейс. Такие сообщения на рисунке 2 показаны двойными стрелками. Другими словами, один и тот же механизм обмена IPMI сообщениями используется во всех интерфейсах, объявленных в стандарте IPMI, просто каждый интерфейс дополнительно «оборачивает» IPMI сообщение в свои специфичные заголовки, которые разнятся в зависимости от типа транспорта.

Обмен IPMI сообщениями использует протокол запроса/ответа. Сообщения с запросом считаются «командами». Например, существует набор команд связанных с контролем датчиков, с событийными командами, командами шасси и так далее. Такое функциональное группирование упрощает процесс организации и управления командами[2].

Системные интерфейсы. IPMI определяет три системных интерфейса, которые используется системным ПО для передачи сообщений к BMC. Чтобы поддерживать разные микроконтроллеры, IPMI предоставляет возможность выбора используемых системных интерфейсов.

Системный интерфейс размещается на системной шине, к которой имеет доступ основной процессор. Представленные в этом пункте интерфейсы могут быть реализованы посредством взаимодействия через I/O порты или общую память. Таким образом системный интерфейс может быть размещен на PCI, LPC или на какой-либо проприетарной шине:

– Keyboard Controller Style (KCS) – принцип работы этого интерфейса соответствует тому, что используется в микроконтроллере Intel 8742 Universal Peripheral Interface. Данные передаются через KCS с использованием побайтного рукопожатия. Этот интерфейс требует для своей работы специализированного аппаратного обеспечения, встроенного в некоторые коммерческие микроконтроллеры.

– System Management Interface Chip (SMIC) – интерфейс, являющийся альтернативным решением для разработчика, желающего использовать в своей системе BMC, не имеющий специальной аппаратной поддержки, требуемой для KCS. Здесь для взаимодействия используются три I/O порта, которые могут быть реализованы с использованием простого ASIC, FPGA или других логических решений. Подобно KCS, SMIC также использует побайтные рукопожатия для передачи данных.

– Block Transfer (BT) – интерфейс, предоставляющий лучшую производительностью, чем предыдущие. В отличие от них, здесь используются уже поблочные рукопожатия. Также, как и в SMIC, BT использует три I/O порта.

– SMBus System Interface (SSIF) – интерфейс, требующий для своей работы доступа BMC к SMBus контроллеру. Является самым нетребовательным к аппаратной части интерфейсом, но в то же время самым низко производительным.

Прочие интерфейсы. В дополнение к системным интерфейсам и к IPMB, обмен IPMI сообщениями может производиться через следующие интерфейсы:

– Serial/Modem Interface – определяет как IPMI сообщения могут быть отправлены к и от BMC через последовательный порт или внешнее модемное соединение.

– LAN Interface – определяет как IPMI сообщения могут отправлять по сети с помощью RMCP (Remote Management Control Protocol) датаграмм, такой способ называется также «IPMI over LAN». Кроме того, здесь определяются специфические возможности конфигурации BMC, такие как, например, установка или смена IP-адреса.

Обзор системы ASUS iKVM

ASUS iKVM – это IPMI 2.0 совместимое средство для удаленного администрирования серверов в режиме реального времени. iKVM предоставляет возможность отслеживания состояния и конфигурации оборудования, удаленного управления сервером, обновления BIOS, операционной системы и другого ПО.

Каждая из версий программного обеспечения совместима со своим BMC микроконтроллером. Так, ПО ASMB7-iKVM предназначено для работы с ASPEED AST2300, а ПО ASMB8-iKVM предназначено для работы ASPEED AST2400.

В качестве исследуемой системы было выбрано ПО ASMB9-iKVM, базирующееся на микроконтроллере ASPEED AST2500, так как оно является наиболее современным и актуальным [3].

Архитектура BMC ASPEED AST2500

Схема с изображением аппаратного обеспечения AST2500 показана на рисунке 3.

В состав BMC ASPEED AST2500 входят следующие компоненты:

– 800 МГц ARM11 процессор;

– DDR3/DDR4 SDRAM с 16-битной шиной данных.

– отдельная SPI флеш память;

– PCIe VGA контроллер;

– отдельный сетевой интерфейс Ethernet с RJ-45 разъемом.

Для удаленного управления ASPEED AST2500 используются следующие интерфейсы (

Рис):

– контроллер Ethernet для реализации сетевого подключения к АРМ администратора;

– контроллер USB 1.1 для локального подключения клавиатуры и мыши;

– виртуальный контроллер USB 2.0 для эмуляции носителя данных;

– VGA контроллер для локального подключения монитора.

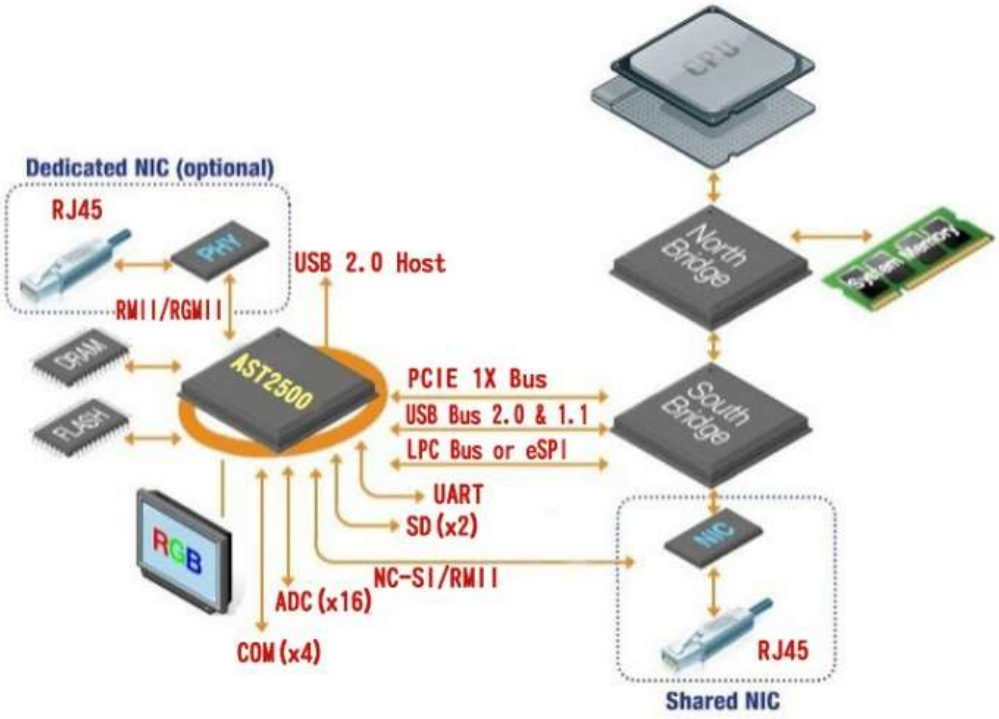

Рисунок 3 – Состав AST2500

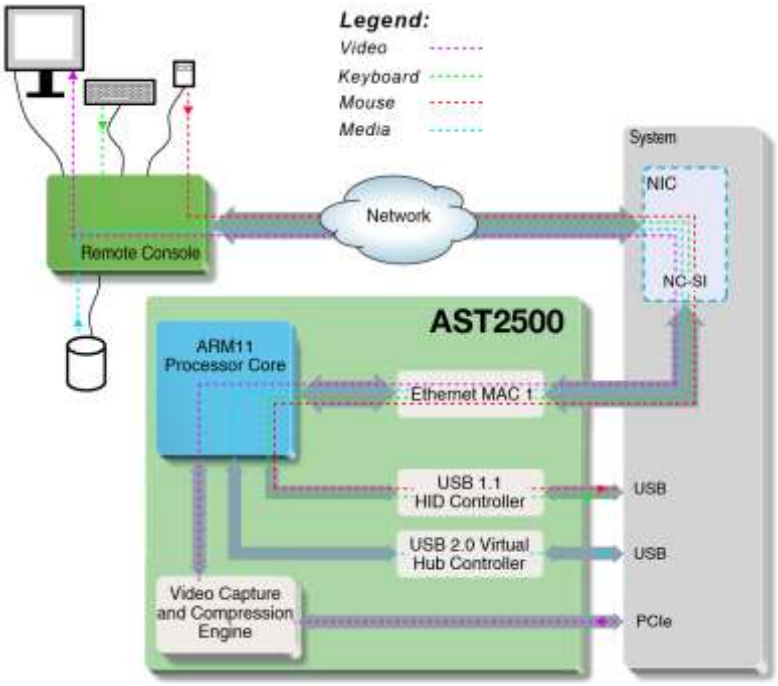

Рисунок 4 – Реализация удаленного управления посредством AST2500

Функциональные возможности ASUS iKVM

В перечень основных функциональных возможностей iKVM входят.

– IPMI 2.0 функционал:

1) KCS интерфейс (Keyboard Controller Style);

2) LAN интерфейс с поддержкой протокола RMCP+;

3) мониторинг системных событий;

4) отслеживание состояния датчиков (SDR);

5) Field Replaceable Unit (FRU);

6) удаленное управление питанием сервера, перезагрузка;

7) поддержка Serial over LAN;

8) поддержка аутентификации типа RAKP-HMAC-SHA1;

9) шифрование (AES);

10) фильтрация событий;

11) реагирование на события определенного типа.

– Отдельная I2C шина:

1) автоматическое отслеживание датчиков (температура, напряжение, скорость вращения вентилятора, регистрация событий).

– Поддержка PMBus и PSMI (Power Supply Management Interface).

– Веб-интерфейс:

1) отслеживание датчиков и журналов; конфигурация BMC и LAN;

2) поддержка HTTPS;

3) многопользовательская система привилегий;

4) обновление прошивки BMC;

5) SSH (Secure Shell);

6) поддержка Active Directory, Lightweight Directory Access Protocol (LDAP);

7) KVM интерфейс.

– Система уведомлений о состоянии компонентов СВТ:

1) фильтрация и реагирование на события (Platform Event Filtering);

2) протокол SNMP;

3) уведомления по e-mail;

4) самодиагностирующиеся светодиодные индикаторы для отображения состояния оборудования;

5) поддержка мониторинга состояния центрального процессора, оперативной памяти, ПЗУ;

– Удаленное обновление BIOS.

– Поддержка виртульных медиа-устройств:

1) возможность подключить два удаленных хранилища (USB/CD-ROM/DVD).

– Удаленная установка основной операционной системы:

1) удаленное монтирование CD для установки ОС;

2) веб-интерфейс, поддерживающий виртуальные устройства, виртуальные директории, монтирование ISO образов.

– Поддержка SNMB MIB (виртуальной базы данных, используемой для управления объектами в сети).

Исследование внутренней архитектуры и особенностей ПО ASUS iKVM

Структура прошивки и особенности ПО

В настоящий момент доступна версия ASMB9-iKVM 1.14.1 (сентябрь 2019 года). Операционная система, используемая в iKVM – Embedded Linux.

Образ прошивки представляет из себя набор разделов, каждый из которых имеет свой тип и предназначение и соответствующий набор заголовков, указывающих на разделы. Заголовки не имеют определенного постоянного места, они разнесены по всему образу. Смещение до каждого заголовка от начала образа выровнено по границе 256 байт. Формат заголовков представлен на рисунке 5.

<table>
<tr><td>0</td><td colspan="3">Signature</td><td colspan="2">0x400801</td><td colspan="2">Unknown</td></tr>
<tr><td>16</td><td colspan="2">Header offset</td><td colspan="2">Unknown</td><td colspan="3">Name</td></tr>
<tr><td>32</td><td>Unknown</td><td>Type</td><td>Unk</td><td colspan="2">Body offset</td><td>Size</td><td>Unknown</td></tr>
<tr><td>48</td><td>Unknown</td><td colspan="2">CRC32</td><td colspan="3">Unknown</td><td>End signature</td></tr>
</table>

Рисунок 5 – Формат заголовка раздела

Заголовок имеет размер, равный 64 байтам и включает в себя следующие поля:

– сигнатура заголовка;
– смещение данного заголовка;
– имя соответствующего раздела;
– тип раздела;
– смещение самого раздела;
– размер раздела;
– контрольная сумма раздела (CRC32);
– сигнатура конца заголовка.

Известны следующие типы разделов.

Стартовый раздел (Boot) – раздел со стартовым кодом, которому в первую очередь передается управление при начале загрузки системы. Его задача состоит в том, чтобы проверить целостность остальных разделов, произвести начальную инициализацию системы и передать управление ядру. Стартовый раздел располагается по нулевому смещению.

Раздел с информацией о системе – несет в себе общую информацию о системе, такую как версия, дата и время сборки прошивки, идентификатор

продукта. Структура раздела: массив, элементами которого являются пары ключ-значение.

Ядро ОС – раздел в котором находится непосредственно ядро операционной системы Linux. В версии прошивки 1.14.1 ядро версии 3.14.17.

Rootfs – раздел, в котором находится корневая файловая система, к которой впоследствии будут монтироваться все необходимые дополнительные разделы.

Дополнительный раздел – раздел, несущий в себе какие-либо данные или программное обеспечение, необходимое для обеспечения функционала, предоставляемого iKVM.

Образ прошивки состоит из разделов, представленных на рисунке 6.

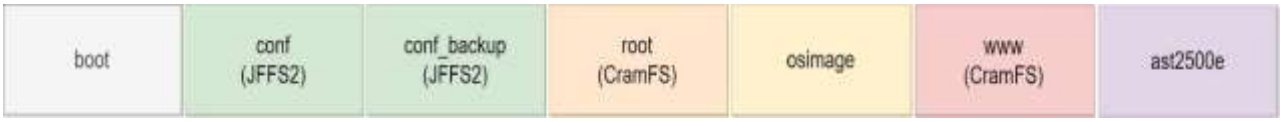

Рисунок 6 – Разделы прошивки

Описание разделов:

– boot раздел – стартовый раздел;

– conf – раздел, содержащий внутренние файлы конфигурации встроенного ПО, конфигурационные файлы, подконтрольные администратору системы и системные журналы событий;

– conf_backup – полная копия раздела conf;

– root – раздел с корневой файловой системой Linux (rootfs);

– osimage – ядро Linux;

– www – раздел, в котором находится ПО, необходимое для работы сервисов, предоставляемых веб-интерфейсом и непосредственно самого веб-интерфейса (html и css файлы, js скрипты, исполняемые на Java машине jar файлы);

– ast2500e – информация о прошивке.

Conf разделы представляют из себя файловую систему JFFS2 (Journaling Flash File System version 2), разделы root и www являются CramFS (Compressed ROM File System) файловыми системами. Все файлы, находящиеся в www, также дополнительно сжаты в gzip (GNU zip).

Механизм обновления прошивки

Процесс обновления прошивки в общем виде и участвующие в нем компоненты представлены на рисунке 7.

Обновление происходит следующим образом:

1. Существует два варианта обновить прошивку: по сети и локально. В случае обновления по сети используется веб-интерфейс. Веб-интерфейсу

предоставляется API, через которое реализуется основная часть доступного функционала. На стороне BMC за предоставление API отвечает компонент spx_restservice, которому перенаправляются все запросы, пришедшие от веб-интерфейса на адрес «/api».

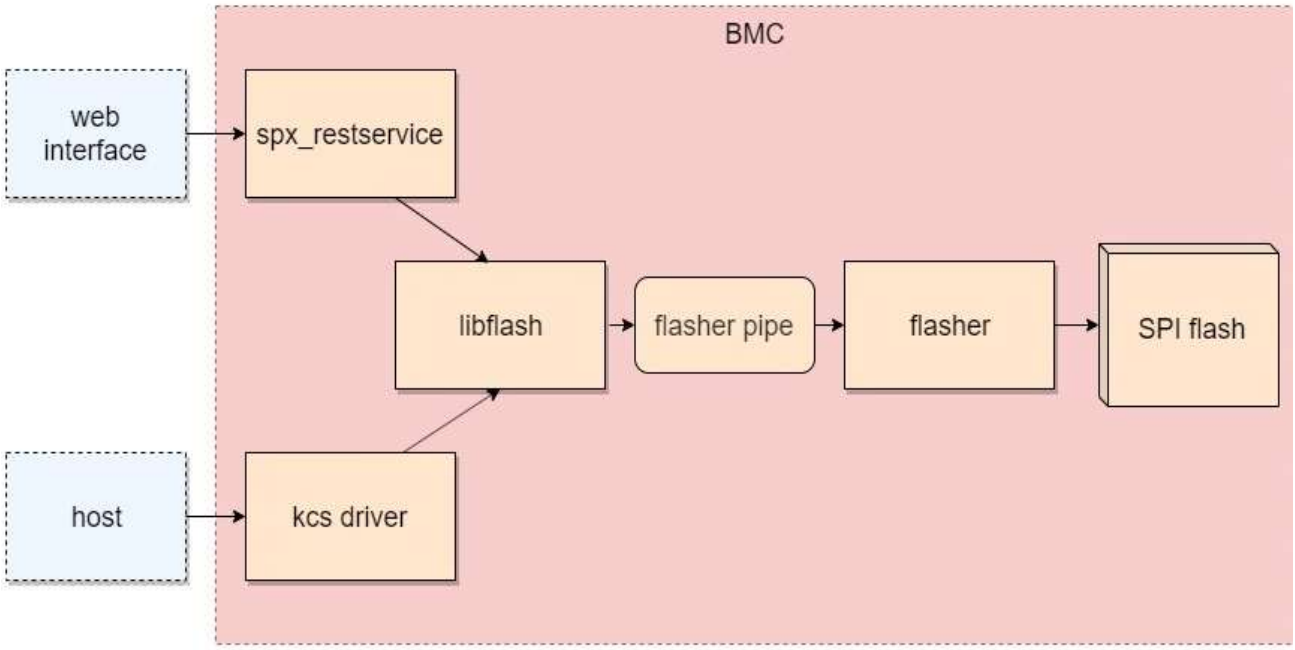

Рисунок 7 – Процесс обновления прошивки

В случае локального обновления образ прошивки передается посредством KCS интерфейса с помощью предоставляемых для этого компанией ASUS утилит. На стороне BMC для предоставления KCS используется модуль ядра «kcs.ko».

2. Для осуществления прошивки используется библиотека libflash. Она, в свою очередь, взаимодействует с компонентом flasher, который проверяет корректность, целостность и опционально криптографическую подпись образа, после чего осуществляет запись образа на SPI flash.

Описание компонента flasher

Flasher взаимодействует с другим процессами, желающими работать с SPI flash, посредством специальных команд. Всего реализовано 15 типов команд, которые позволяют перезаписать или считать данные SPI flash, верифицировать образ прошивки, получить или изменить определенные настройки.

Подробнее остановимся на команде FLSH_CMD_VERIFY_IMAGE, с помощью которой происходит верификация образа прошивки. iKVM поддерживает два вида прошивок: подписанные криптографически и неподписанные.

В конце подписанной прошивки находится криптографическая информация, позволяющая проверить ее корректность с помощью алгоритма RSA. Открытая часть ключа RSA, нужная для проверки подписи, находится в разделе conf текущей прошивки. Помимо криптографической верификации также проверются контрольные суммы заголовков и CRC32 суммы разделов.

Если прошивка не подписана (ее длина кратна 128), проверяются только контрольные суммы заголовков и разделов.

Поддержка неподписанных прошивок определяется опцией SPX_FEATURE_SIGNED_HASHED_IMAGE_SUPPORT, которая задается во внутренних конфигурационных файлах раздела root, недоступных для редактирования даже администратору системы.

В исследуемой версии прошивки такая опция отключена, то есть, поддерживаются неподписанные образы. Было обнаружено, что все официальные версии прошивок, размещенные на сайте производителя за 2019 год, также не содержат криптографической подписи.

Таким образом, в данной работе проведен анализ основных положений и интерфейсов, объявленных в IPMI спецификации, кроме того проведено исследование безопасности конкретной реализации IPMI системы ASUS iKVM. Можно сделать вывод о недостаточном уровне защищенности рассмотренной реализации. Данная система обладает рядом недостатков, основным из которых является отсутствие криптографической проверки образа обновления прошивки, что может привести к внедрению злоумышленником вредоносного программного обеспечения в систему iKVM.

Список литературы

1. PMI Specification, V2.0, Rev. 1.1 [Электронный ресурс]. URL: https://www.intel.com/content/www/us/en/products/docs/servers/ipmi/ipmi-second-gen-interface-spec-v2-rev1-1.html (дата обращения 10.11.2019).
2. ASMB9-iKVM Server Management Board User Guide [Электронный ресурс]. URL: https://dlcdnets.asus.com/pub/ASUS/server/accessory/ ASMB9/E15496_ASMB9-iKVM_UM_V2_WEB.pdf (дата обращения: 10.11.2019).
3. Sold Down the River [Электронный ресурс]. URL: http://fish2.com/ipmi/river.pdf (дата обращения: 10.11.2019).

УДК 004.056

Разработка концепции системы автоматического анализа сетевого трафика на основе моделей самообучения и использования статистических методов классификации данных

Д. Д. Бурзунов, студент группы ИБ-1801,
Г. А. Крайковский, студент группы ИБ-1801,
Санкт-Петербургский Государственный Экономический Университет

Люди обмениваются все большим количеством информации. Из-за этого способы ее анализа быстро устаревают, поэтому используемые при анализе алгоритмы постоянно совершенствуются. Это необходимо для поиска угроз в передаваемой информации. Сегодня программисты создают алгоритмы, работающие без участия человека – это экономит силы и время, а также исключает ошибки, совершаемые людьми во время работы.

В интернете информация передается в виде сетевого трафика. Сетевой трафик зачастую содержит в себе угрозы, которые искажают передаваемую информацию. Такой трафик называется вирусным. Вирусный трафик разнообразен: способы нанести ущерб информации становятся вариативнее и сложнее, поэтому программисты пытаются создавать алгоритмы, способные самостоятельно искать в трафике вирусную составляющую.

Суть работы таких алгоритмов заключается в следующем. В их основу закладывается исходная информация о том, чем характерен вредоносный трафик. На основе этих критериев алгоритм находит предположительные угрозы. Изучая отобранные образцы, алгоритм ищет сходства между ними, после чего снова начинает искать вредоносный трафик, используя новые параметры. Такие алгоритмы называются самообучающимися.

Из-за своих преимуществ, современные самообучающиеся алгоритмы устроены подобно нейронной сети – математической модели, построенной по принципу функционирования сетей нервных клеток живого организма. Этот принцип применяется на промышленном уровне уже второй десяток лет: его эффективность подтверждена временем. Поэтому цель данной работы – создать программу, которая будет определять угрозы в получаемом сетевом трафике благодаря алгоритмам, построенным по принципам нейросети.

Рассмотрим предмет и объект исследования.

Объект исследования – сетевой трафик, том числе вредоносный.

Предмет исследования – анализ сетевого трафика с использованием модели нейронных сетей для обнаружения угроз.

Представим механизм работы создаваемой программы (рисунок 1).

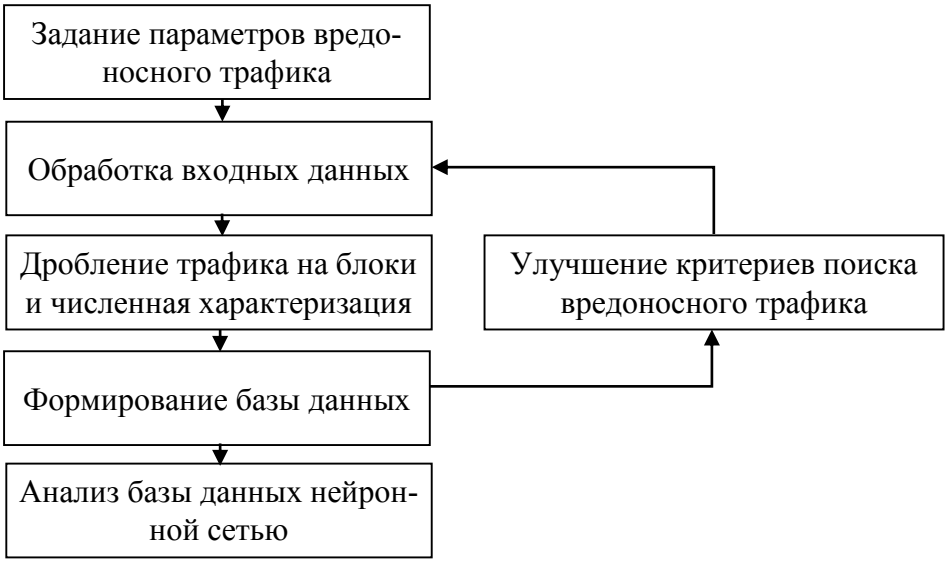

Рисунок 1 – Структура программы

1. Программа получает параметры, отделяющие вредоносный трафик от безвредного. Рассмотрим два способа формирования таких параметров. Первый способ – задание отличительных признаков потенциально вредоносного трафика человеком напрямую. Второй способ заключается в том, что перед началом работы алгоритм получает трафик и информацию о том, является ли он вредоносным. Анализируя разницу между вредоносным и безвредным трафиком, алгоритм самостоятельно формирует закономерности, присущие этим двум группам. Последний способ имеет недостаток – эффективность его использования зависит от трафика, который был проанализирован алгоритмом изначально. Рассматриваемая нейросеть задействует первый способ формирования таких параметров.

2. Программа принимает входные параметры для обработки.

3. Программа делит изучаемый трафик на блоки и численно характеризует каждый из них в соответствии с критериями вредоносности трафика, которыми она располагает. Процесс нужен для удобства статистического анализа блоков трафика в дальнейшем.

4. Из сформированных в п.3 наборов чисел формируется база данных.

5. Нейронная сеть анализирует данные, используя методы кластеризации и классификации.

6. На основе исследований, проведенных в п.5, нейросетью формируются новые закономерности, проявляющиеся у вредоносного трафика. Добавление новых критериев к списку имеющихся. Повторение п.2-6.

В качестве исходных параметров выбраны общие характеристики трафика, анализ которых показывает его вредоносность:

– максимальная скорость передачи данных;
– средняя скорость передачи данных;
– минимальная скорость передачи данных;

– коэффициент пульсации трафика (отношение пиковой скорости на малом интервале времени к средней скорости обмена данными на длительном интервале времени);

– доля потерянных ячеек;

– задержка передачи ячеек;

– вариация задержки ячеек;

– используемый протокол;

– «джиттер» (случайная задержка распространения пакета).

Для выполнения п.5 используются два алгоритма статистического и кластерного анализа.

Первый алгоритм – алгоритм Expectation maximization (EM). В методе EM предполагается, что кроме известных параметров трафика, присутствуют и неизвестные, относящиеся к распределению по кластерам. Такие неизвестные формируют группу, обобщенную неизвестным критерием, а наблюдается только деятельность таких неизвестных. Задача алгоритма EM сводится к оценке таких неизвестных. В общем случае предполагается, что такая группа – результаты наблюдения, распределенные нормально, тогда для их характеристики применяется многомерная функция Гаусса. В этом случае задача сводится к определению распределений, к которым принадлежит каждый конкретный набор чисел [4].

Второй алгоритм – алгоритм k-средних. Это значит, что набор чисел, характеризующий конкретный блок сетевого трафика, относится только к одному кластеру. Кластеризация методом k-средних – метод определения принадлежности элементов кластерам с помощью минимизации разницы между элементами кластера и максимизации расстояния между кластерами. Слово «средние» в названии метода относится к центроидам кластеров. Центроид – числовой набор, который выбирается произвольно, а затем итеративно уточняется, пока не начинает представлять собой истинное среднее всех наборов кластера. «k» означает произвольное количество точек, используемых для формирования начальных значений процесса кластеризации.

Алгоритм k-средних вычисляет квадраты евклидовых расстояний между записями числовых наборов в кластере и вектор, представляющий собой среднее значение числового набора кластера. Метод сходится, выдавая окончательный набор из k кластеров, когда упомянутая сумма минимизирована. Алгоритм k-средних назначает каждому набору чисел ровно один кластер и не допускает неопределенности в принадлежности точки кластеру. Принадлежность к классу выражается расстоянием от центроида. Метод k-средних хорошо работает, если данные делятся на компактные, сферические группы [4].

Данная система обнаружения вредоносного трафика находится на этапе разработки и, на взгляд авторов, имеет широкие перспективы использования.

Список литературы

1. Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О. Обзор задач и методов их решения в области классификации сетевого трафика [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/obzor-zadach-i-metodov-ih-resheniya-v-oblasti-klassifikatsii-setevogo-trafika (дата обращения: 15.10.2019).
2. Шыхалиев Р.Г. Анализ и классификация сетевого трафика компьютерных сетей [Электронный ресурс]. URL: https://jpit.az/storage/files/article/b61aeb69dd6a7e2a8ee2a22285b321bd.pdf (Дата обращения: 14.10.2019).
3. Щербакова Н.Г. Анализ ip-трафика методами Data Mining. Проблема классификации [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/analiz-ip-trafika-metodami-data-mining-problema-klassifikatsii (дата обращения: 18.10.2019).
4. Технический справочник Майкрософт по алгоритмам кластеризации [Электронный ресурс]. URL: msdn.microsoft.com/ru-ru/library/cc280445.asp (дата обращения: 15.10.2019).
5. Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Методы и модели анализа данных: OLAP и Data Mining – СПб.: БХВ-Петербург, 2004. – 336 с.

УДК 004.056.2

Обеспечение целостности системных ресурсов в операционных системах Windows и Linux

И. Н. Васильева, к.ф.-м.н., доцент
Санкт-Петербургский Государственный Экономический Университет

Поддержание целостности системных ресурсов крайне важна как для устойчивой и надежной работы самой операционной системы (ОС), так и для обеспечения доверия к ней. Подмена исполняемых системных файлов или файлов конфигураций позволяет нарушителям выполнять произвольные несанкционированные действия, а также скрывать следы своего присутствия в системе и активно противодействовать средствам защиты информации. Например, такой тип вредоносного программного обеспечения (ПО), как руткиты, поставляют ложную информацию – как правило, они скрывают некоторые файлы на диске или работающие процессы. Чаще всего речь идет о файлах, установленных нарушителем после взлома системы. Кроме того, существует возможность модификации ОС таким образом, чтобы она автоматически подменяла данные в некоторых секторах диска (например, при попытках антивирусного сканирования).

Поэтому с точки зрения безопасности ОС крайне важно обеспечить возможность проверки целостности системных компонент и, в случае необходимости, их восстановления. Методические документы ФСТЭК России «Профили защиты операционных систем» [9] включают (в зависимости от типа и класса ОС) следующие функциональные требования безопасности:

– контроль целостности компонентов ПО, разрешенного для запуска, и реагирование на попытки запуска компонентов ПО, целостность которых была нарушена;

– возможность тестирования (самотестирования) функций безопасности ОС, проверки целостности ПО ОС и целостности данных (параметров) ОС;

– возможность обеспечения восстановления штатного режима функционирования ОС;

– возможность возврата ОС при сбоях и отказах к безопасному состоянию в автоматизированном режиме;

– возможность восстановления объектов ОС из резервных копий, созданных с использованием ОС, и использования ассоциированных с ними атрибутов безопасности.

Подсистема целостности ОС может использовать разные концепции. Один из подходов рассматривает целостность как принципиальную неизменяемость файлов, так что в файл не могут быть внесены какие-либо изменения. Концепция неизменяемых файлов реализована, например, в ОС BSD, такие файлы могут быть изменены только в административном однопользовательском режиме. ОС Android хранит все свои системные файлы в разделе, который монтируется только для чтения во время нормальной работы, изменения же могут быть внесены только программой восстановления во время загрузки. Неизменные системы хотя и обеспечивают большую целостность, однако затрудняют нормальную установка или исправление системных компонентов. На сходных принципах базируется и система защиты ресурсов Windows (WRP), однако здесь доступ к критическим системным файлам оставлен для системы обновления и восстановления.

Другой подход заключается в расчете и хранении эталонных значений (значений бесключевых хэш-функций, цифровых подписей или кодов аутентификации MAC, HMAC), позволяющих проводить проверку целостности файлов. При этом надежность такого подхода во многом определяется степенью защиты хранения эталонов.

Большинство развитых ОС сочетают оба подхода для обеспечения достаточного уровня контроля целостности системы наряду с гибкостью ее обновления и исправления. Существует три основных направления обеспечения целостности критических системных объектов:

– защита системных файлов и данных (параметров, конфигураций) во время работы ОС;

– защита от автономных атак (когда ОС не активна);

– контроль целостности системных объектов и их восстановление в случае обнаружения несанкционированного изменения.

Защита критически важных системных файлов во время работы ОС решается путем ограничения доступа к ним. В ОС Linux используется стандартная модель безопасности, в которой для изменения системных файлов могут быть произведены только от лица root. Дополнительно могут быть включены и настроены списки доступа ACL наподобие разрешений дискреционной защиты Windows, однако по умолчанию эта возможность в Linux системах отключена.

В ОС Windows предусмотрена защита системных файлов WRP (Windows Resource Protection) для версий ОС, начиная с Vista, и WFP (Windows File Protection) для старых версий ОС. WRP предотвращает замену основных системных файлов, папок и разделов реестра, установленных как часть ОС. Windows Resource Protection работает, устанавливая дискретные списки доступа (DACLs) и ACL для защищаемых объектов. Владельцем таких объектов является субъект SYSTEM (Система), а разрешение на чтение-запись допускается лишь процессам, использующим службу Установщик модулей Windows (Windows Modules Installer – TrustedInstaller.exe).

Ограничения WRP базируются на функциональных возможностях обязательного контроля целостности (Mandatory integrity control, MIC), доступных начиная с Windows Vista. Когда пользователь входит в систему, ему присваивается идентификатор целостности (integrity SID). Он содержит метку целостности, которая определяет уровень доступа маркера пользователя (token), и, следовательно, указывает уровень полномочий, которых этот пользователь может достигнуть. Во время проверки прав доступа пользователю разрешается модифицировать или удалять объект, если присвоенный ему уровень целостности доминирует (то есть это число больше уровня целостности объекта или равно ему). В противном случае попытка доступа будет отклонена.

Определено пять уровней целостности [8]:

– ненадежный (untrusted) – блокирует большинство операций записи;

– низкий (low) – блокирует запись большинства системных объектов;

– средний (medium) – используется обычными приложениями;

– высокий (high) – используется приложениями, запущенными с правами администратора;

– системный (system) – используется системными службами и процессами.

Обычные пользователи имеют средний уровень, при повышении уровня полномочий до администратора они получают высокий. Настройки прав доступа для объектов, защищенных механизмом WRP, таковы, что доступ к ним имеет только сервис TrustedInstaller, а все остальные учетные записи, включая SYSTEM, имеют право только на чтение и исполнение. Поэтому даже администраторы не имеют прав полного доступа к системным файлам.

Однако система контроля целостности не может защитить файлы ОС от автономных атак. Если компьютер был загружен с другого экземпляра ОС, например, с Live CD, или при непосредственном физическом доступе к носителю информации, ограничения доступа будут не активны и защищенные файлы ОС могут быть изменены.

Средства контроля целостности на уровне логических блоков диска, предлагаемые рядом отказоустойчивых файловых систем, таких как ZFS и BtrFS компании Oracle или ReFS от Microsoft, оказываются в этом случае недостаточными, так как расчет контрольных значений осуществляющие на основе алгоритмов контрольных сумм (CRC или бесключевых хэш-функций), не защищенных паролем. Таким образом, у нарушителя остается возможность подмены как самой информации, так и соответствующих контрольных сумм. Для решения этой проблемы требуется использование средств криптографической защиты информации, например, криптографических контрольных сумм, значения которых невозможно рассчитать без знания секретной информации (ключа), – кодов аутентификации MAC, представляющих собой особые режимы работы блочных шифров, либо HMAC, совмещающих использование хэш-функций и ключевой информации.

В качестве традиционного средства защиты от автономных атак рассматривается полнодисковое шифрование носителей информации, в том числе, и системных дисков. Полнодисковое шифрование не позволяет нарушителю целенаправленно менять хранимую на диске информацию и эффективно контролировать изменения, однако сохраняется возможность изменения «вслепую» на уровне отдельных секторов и даже байтов. Таким образом, полнодисковое шифрование не может гарантировать отсутствия неконтролируемых изменений на диске, в том числе и в результате сбоев и отказов оборудования. При этом эффективно локализовать местоположение модифицированных данных не всегда представляется возможным.

Требование одновременного обеспечения конфиденциальности и целостности защищаемой информации приводит к необходимости использования аутентифицированного шифрования (Authenticated Encryption, AE). Следует отметить, что контроль целостности блоков данных, как отдельная функция, так и в составе аутентифицированного шифрования, требует дополнительных накладных расходов на хранение присое-

диненных данных (например, используемых в проверках контрольных сумм), которые для носителей большого размера могут оказаться весьма существенными. Например, для пустого диска объемом 10 Гб, отформатированного в файловой системе ReFS, дисковое пространство, выделенное под контрольные данные, составит около 700 Мб (7%). А накладные расходы на хранение криптографической контрольной суммы при использовании полнодискового аутентифицированного шифрования geli в ОС FreeBSD с HMAC-SHA256 и размере сектора 4096 бит составляют порядка 11% доступного объема диска [11].

Помимо инструмента geli в ОС FreeBSD, возможность полнодискового аутентифицированного шифрования или только контроль целостности содержимого диска поддерживается в ОС Linux (dm-integrity и LUKS2) в качестве экспериментальной. В настоящее время эти функции не рекомендованы для промышленного использования.

Высокие накладные расходы при сквозном контроле целостности средствами файловых систем или полнодискового аутентифицированного шифрования/ криптографического контроля целостности, а также недостаточная проверенность как реализаций, так и самих алгоритмов полнодискового аутентифицированного шифрования, являются факторами, сдерживающими практическое применение указанных средств.

Поэтому на современном этапе актуален подход, заключающийся в обеспечении возможности периодической проверки и восстановления, в случае необходимости, критически важных для работы системы файлов. Такой подход реализован, в частности, в ОС Windows.

Система защиты ресурсов Windows (WRP) включает два инструмента проверки целостности защищенных системных файлов – SFC (System File Checker) и DISM (Deployment Image Servicing and Management), работающих в режиме командной строки, а также использующую DISM команду Repair-WindowsImage в Windows PowerShell [2, 7].

Если есть основания полагать, что системные файлы ОС были повреждены или изменены, в командной строке, запущенной от имени администратора, следует выполнить `sfc /scannow`. Найденные ошибки целостности будут автоматически исправлены с выдачей подтверждающего сообщения. Также имеется возможность проверить целостность конкретного системного файла (`sfc /scanfile= путь_к_файлу`). SFC не может исправить ошибки целостности для активных системных файлов, которые используются в настоящий момент времени. В таком случае можно запустить SFC через командную строку в среде восстановления (в безопасном режиме). Существует и возможность запуска только проверки системных файлов без их исправления (`sfc /verifyonly` или `/verifyfile`).

WRP копирует файлы, необходимые для перезапуска Windows, в каталог кэша, расположенный по адресу `%Windir%\winsxs\Backup`. Размер

каталога кэша и список кэшируемых файлов не может быть изменен. После установки ОС WFP копирует проверенные версии системных файлов (.dll, .exe, .ocx и .sys и некоторые шрифты TrueType) в хранилище `%systemroot%\system32\dllcache`, местоположение и размер которого могут настраиваться. WFP будет добавлять файлы в хранилище до тех пор, пока его размер не достигнет заданного предела. Для восстановления защищенного файла, отсутствующего в хранилище, WFP обратится к источнику установки.

Восстановление системных файлов приводит к сбросу некоторых пользовательских настроек (например, замененных значков в Проводнике и пр.), изменения, заданные политиками, не сбрасываются.

Инструмент DISM позволяет выявить и исправить проблемы с хранилищем системных компонентов Windows (начиная с 8). Это может оказаться необходимым в случае, если SFC не может выполнить восстановление системных файлов, несмотря на найденные повреждения.

В командной строке, запущенной от имени администратора, следует выполнить:

– для получения информации о состоянии и наличии повреждений компонентов Windows: `dism /Online /Cleanup-Image /CheckHealth`

– для проверки целостности и наличия повреждений хранилища компонентов: `dism /Online /Cleanup-Image /ScanHealth`

– для проверки и автоматического восстановления системных файлов Windows: `dism /Online /Cleanup-Image /RestoreHealth`

Результаты выполнения команд SFC и DISM протоколируются. Если восстановление системных файлов не удается выполнить в автоматическом режиме с помощью инструментов SFC и DISM, в файле журнала можно посмотреть, какие конкретно системные объекты были повреждены, а затем восстановить их вручную, скопировав из источника установки (предварительно потребуется сменить владельца файла/ папки и задать соответствующие разрешения доступа).

Еще одно средство проверки системных файлов – инструмент проверки подписи файла (File Signature Verification, Sigverif.exe). Все входящие в состав Windows драйверы и системные файлы (начиная с Vista) должны иметь цифровую подпись, свидетельствующую, что они протестированы в лаборатории WHQL (Windows Hardware Quality Labs) и могут быть использованы с текущей версией Windows. Это позволяет сохранить целостность и стабильность ОС и быстро найти поврежденные или измененные файлы.

В старых версиях ОС Windows (XP, 2000 и Server 2003) в зависимости от выбранных значений политики «Цифровая подпись драйверов устройств», ОС может либо игнорировать драйверы, не имеющие цифровой подписи, либо выводить предупреждение при их обнаружении, либо не

допускать их установки. В более поздних версиях драйверы и сервисы, загрузка которых осуществляется загрузчиком ОС перед инициализацией ядра, должны иметь цифровую подпись. В 64-разрядных версиях Windows для загрузки любого ПО, работающего на уровне ядра, наличие цифровой подписи обязательно.

Цифровые подписи драйверов, входящих в дистрибутив Windows, хранятся в файлах каталога (catalog files) в папке %SystemRoot%\System32\Catroot. Драйверы подключаемых устройств должны поставляться вместе с их собственными файлами каталога, которые Microsoft предоставляет фирме-разработчику после успешного тестирования на совместимость с Windows [5].

Верификация цифровой подписи файлов служит для поиска установленных на компьютере файлов, не имеющих цифровой подписи. Список подписанных и неподписанных драйверов, обнаруженных программой Sigverif, помещается в файл `Sigverif.txt` вместе с информацией о дате модификации, типе и номере его версии. Файл журнала может располагаться в каталоге Windows или \Users\Public\Documents\ (для Windows 10).

В Linux системах возможна проверка целостности установленных в системе пакетов. Это позволяет убедиться в том, что файлы, установленные из пакета, не были изменены после инсталляции. В Red Hat Linux и других дистрибутивах, использующих для установки пакетов RPM (RPM Package Manager) для этих целей используется опция `--verify` (`-V`) одноименной команды: `rpm --verify --all` (или `rpm -Va`). Можно выполнить также проверку файлов отдельного пакета или пакета, которому принадлежит указанный файл. При проверке пакета информация об установленных из пакета файлах сравнивается с информацией из оригинального пакета. Помимо прочего, при такой проверке проверяется размер, сумма MD5, разрешения, тип, владелец и группа владельца каждого файла. Результатом выполнения команды будет список кодов найденных ошибок с указанием полного пути файла.

Пакет, как правило, подписывается разработчиком и содержит контрольные суммы устанавливаемых файлов (в .deb пакетах подписываются файлы, содержащие список контрольных сумм). Для проверки целостности файла RPM-пакета используется опция `--checksig` (или `-K`) команды rpm. Для проверки цифровой подписи пакетов требуется открытый ключ. Открытые ключи для проверки подписи, как правило, загружаются автоматически при установке из дистрибутива.

В Linux Debian/ Ubuntu и подобных дистрибутивах с dpkg используется утилита debsums, которая должна быть предварительно установлена на компьютер. Debsums сравнивает хэш-коды md5 файлов с контрольными значениями из каталога /var/lib/dpkg/info.

Например, проверка целостности всех установленных файлов с выводом лишь измененных может быть произведена командой `debsums --changed --all` (`debsums -ca`).

Обе утилиты используют в качестве эталонов внутреннюю базу соответствующего установщика пакетов (rpm или dpkg), хранящуюся на компьютере. Поскольку в качестве контрольных сумм, как правило, используются значения бесключевых хэш-функций, эталоны, вообще говоря, могут быть изменены наряду с самими файлами. Однако наличие цифровой подписи пакета позволяет проверить неизменность эталонной информации.

При обнаружении изменений, пакеты следует переустановить, например, в Debian/ Ubuntu это можно сделать командой

```
apt-get install --reinstall $(dpkg -S $(debsums -c) | cut -d : -f 1 | sort -u)
```

Однако такой метод не подходит для системных файлов.

Контроль целостности избранных файлов, в том числе и системных, может производиться с помощью сторонних решений, которые доступны в большинстве дистрибутивов Linux.

Monit (https://mmonit.com/monit/) – небольшая утилита для управления и мониторинга процессов, программ, файлов, каталогов и файловых систем в *nux системах. Доступна для большинства Linux дистрибутивов, FreeBSD и OpenBSD, MacOS и Solaris, позволяет работать как в режиме командной строки, так и через веб-интерфейс. Monit записывает события в syslog или свой собственный файл журнала, а также может отправлять уведомления в случае обнаружения изменения контрольной суммы файла, либо добавления новых объектов файловой системы. Monit может выполнять автоматическое восстановление и проводить другие необходимые действия в случае возникновения ошибок.

AIDE (Advanced Intrusion Detection Environment) – утилита проверки целостности файлов (https://aide.github.io/). AIDE создает базу данных контрольных значений файлов в системе, а затем использует эту базу данных в качестве критерия для обеспечения целостности файлов и обнаружения системных вторжений. Для расчета контрольных значений могут использоваться контрольные суммы crc32 или хэш-функции, включая sha256 и sha512. Все обычные атрибуты файла (тип файла, разрешения, индексный дескриптор, Uid, Gid, имя ссылки, размер, количество блоков, количество ссылок, атрибуты времени) также можно проверить на несоответствия. Поддерживаются атрибуты файловой системы Posix ACL, SELinux, XAttrs и Extended. Позволяет использовать регулярные выражения для выборочного включения или исключения файлов и каталогов для мониторинга. AIDE доступен для большинства дистрибутивов Linux, FreeBSD и может работать на любой современной Unix-системе.

Tripwire (https://github.com/Tripwire/tripwire-open-source) – инструмент проверки целостности, который позволяет обнаруживать изменения системных файлов. Проект основан на коде, изначально предоставленном компанией Tripwire в 2000 году. Tripwire включает два основных компонента: политику и базу данных. Политика содержит список всех файлов и каталогов, для которых средство проверки целостности должно сделать снимок, в дополнение к созданию правил для выявления нарушений изменений в каталогах и файлах. База данных состоит из снимка, сделанного Tripwire. Tripwire также имеет файл конфигурации, в котором указывается расположение базы данных, файла политики и исполняемого файла Tripwire. Для файлов политики и конфигурации, а также файлов базы данных и сгенерированных отчетов обеспечивается криптографическая защита (для этих целей предоставляются два криптографических ключа – ключ сайта и локальный ключ). Tripwire работает, периодически сравнивая каталоги и файлы со снимком в базе данных и сообщая о любых изменениях.

Развитый механизм контроля целостности системных файлов ОС Linux – IMA (Integrity Measurement Architecture) [10, 12, 13, 15], доступен для ядра версии 2.6.30 и выше. Технология IMA включена не во все дистрибутивы, поэтому для ее использования может потребоваться пересборка ядра. Однако в дистрибутивах с поддержкой IMA (например, Linux Ubuntu, начиная с версии 14.04) включение IMA требует лишь перезапуска с указанием соответствующей политики в командной строке загрузки. По умолчанию технология IMA отключена, так как требует значительных накладных расходов, в частности, существенно увеличивает время загрузки системы – примерно в 8 раз, по оценкам [14].

Подсистема IMA отвечает за вычисление хэш-значений файлов и программ при их открытии до того, как их содержимое будет доступно для чтения или выполнения, а также поддерживает проверку их соответствия заранее заданному списку и создание отчетов.

Когда система впервые устанавливается в известном доверенном состоянии, записывается список «хороших» значений хеш-функции. Во время обычной работы системы IMA поддерживает список текущих файловых хэшей. Затем этот список можно сравнить с первоначально записанным списком «хороших» хэшей, чтобы обнаружить любые необоснованные изменения. Технология IMA изначально использовалась только для дальнейшей аттестации системы, то есть была пассивным средством защиты информации.

Начиная с версии ядра 3.7 технология IMA дополнена функцией оценки и компонентом EVM (Extended Verification Module), позволяющем блокировать загрузку бинарных данных в случае обнаружения нарушений их целостности. В настоящее время IMA/EVM предоставляют две основные функциональные возможности:

– измерение (хэширование) содержимого файла при обращении к нему и отслеживание этой информации в журнале аудита;

– оценка файлов, которая позволяет запретить доступ к файлу, если результат его измерения или цифровая подпись не соответствуют ожидаемому значению.

Функция измерения IMA используется только для обнаружения потенциально вредоносных изменений в системе, но не для их предотвращения. Функция оценки позволяет предотвратить выполнение или даже чтение ненадежных файлов. Это достигается путем подписания хэша содержимого файла и дальнейшей проверки подписи с использованием криптографии с открытым ключом (RSA).

Использование цифровых подписей подходит только для файлов, которые не должны изменяться во время выполнения, потому что в противном случае подпись необходимо будет пересчитать с использованием закрытого ключа, который не должен храниться в системе по соображениям безопасности. Поэтому подписи, как правило, используют для двоичных файлов, а не для файлов конфигурации.

Если IMA использует только значение бесключевой хэш-функции, защита этого значения производится с помощью EVM. IMA/ EVM хранят хэш-значения или подписи файлов в расширенных атрибутах. Расширенный атрибут IMA хранит данные о фактическом содержимом файла. Расширенный атрибут EVM хранит данные о метаданных файла, такие как владение, биты режима, другие расширенные атрибуты и т. д. EVM создает подписанное хэш-значение или HMAC для указанных метаданных файлов. Использование EVM подписей целесообразно только для редко изменяемых файлов. Расчет HMAC требует использования ключа симметричного шифрования, который может вычисляться на основе вводимого пользователем пароля или храниться аппаратно (например, в доверенном платформенном модуле TPM).

EVM работает только в сочетании с инфраструктурами безопасности, то есть проверка метаданных EVM выполняется только тогда, когда выполняется оценка IMA. Если проверка метаданных не удалась, доступ к рассматриваемому файлу будет отклонен.

IMA/ EVM могут работать на платформах без аппаратного TPM, хотя и без аппаратной гарантии обнаружения компрометации. Преимущество привязки списка эталонных хэш-значений IMA или ключей к TPM состоит в том, что список измерений не может быть скомпрометирован какой-либо программной атакой без возможности обнаружения. Поэтому в доверенной загрузочной системе измерения IMA могут использоваться для подтверждения целостности системы во время выполнения. Оценка IMA при использовании совместно с TPM расширяет концепцию «безопасной загрузки» на запуск файлов доверенной ОС (рисунок 1).

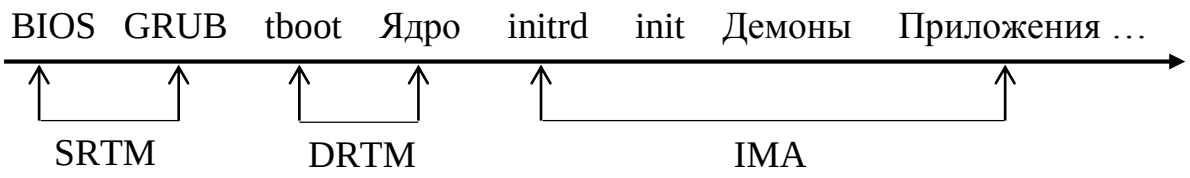

Рисунок 1 – Доверенная загрузка Linux системы
с использованием TPM и IMA

Безопасная и доверенная загрузка ОС

Безопасная загрузка является важным компонентом обеспечения целостности как самой ОС, так и подсистем ее защиты.

Так, например, программная реализация полнодискового шифрования для системных дисков требует прохождения предварительной аутентификации (Pre-Boot Authentication, PBA) для получения от пользователя информации (пароля, ключевого файла), позволяющей разблокировать носитель информации, то есть получить доступ к ключам шифрования данных, хранящимся в зашифрованном виде. Поэтому некоторая часть диска, содержащая модули начальной предаутентификационной загрузки и метаданные, остается незашифрованной. Подмена и модификация загрузочного кода, возможная при физическом доступе к диску, позволяет нарушителю контролировать процесс предаутентификации и, как следствие, получить доступ к зашифрованным данным.

В ОС Windows контроль целостности файлов загрузки обеспечивается использованием встраиваемого в материнскую плату компьютера аппаратного компонента – доверенного платформенного модуля (Trusted Platform Module, TPM), что предполагает, кроме того, жесткую аппаратную привязку зашифрованного носителя. На территории Российской Федерации компьютеры с TPM недоступны из-за экспортных ограничений.

В ОС Linux открытый раздел с файлами загрузчика и конфигураций может быть перенесен на съемный носитель, с которого будет осуществляться загрузка. Кроме того, загрузчик нового поколения Grub2 поддерживает непосредственную загрузку из UEFI с активным Secure Boot [3]. В этом случае можно настроить полное шифрование диска LUKS, включая и раздел /boot. Непосредственная загрузка из UEFI поддерживается в случае, если ядро Linux было скомпилировано с параметром CONFIG_EFI_STUB.

Безопасная загрузка (UEFI Secure Boot) – механизм проверки, обеспечивающий надежность кода, запускаемого микропрограммой. использование UEFI Secure Boot требует, чтобы каждый двоичный файл, запущенный при загрузке, проверялся по известным ключам доверенных поставщиков для идентификации проверенных аппаратных компонентов, микропрограмм и кода загрузчика ОС. Безопасная загрузка позволяет

предотвратить выполнение неподписанного кода на этапе загрузки и выполнения ОС (например, как в ОС Windows, так и в ОС Linux проверяются подписи драйверов/модулей ядра, таким образом, безопасная загрузка не позволяет системе выполнять случайно или преднамеренно измененный код в режиме ядра).

Когда какая-нибудь программа или ОС пытается загрузиться в память компьютера, Secure Boot сравнивает сигнатуру загрузочного кода с ключами, зашитыми непосредственно в BIOS и, если загрузочный код не проходит проверку подписи, загрузка тут же блокируется.

Однако при получении нарушителем физического доступа к компьютеру существует возможность подмены предустановленных ключей. Эта проблема решается при использовании аппаратно защищенного ключевого хранилища, например, TPM.

Доверенный платформенный модуль TPM (Trusted Platform Module) – криптографический сопроцессор, включающий аппаратный генератор случайных чисел и защищенное хранилище ключевой информации. Криптографические ключи никогда не покидают микросхему TPM, поэтому хост-процессор и ОС не могут напрямую обращаться к ним. TPM также участвует в формировании цепочек доверия при загрузке ОС. В этом случае цель использования TPM состоит в обеспечении целостности платформы, то есть в контроле того, что оборудование и ПО, участвующее в процессе загрузки, выполняет строго предопределенные действия до полной загрузки ОС [4].

TPM является пассивным устройством, поэтому все действия по обеспечению целостности выполняются встроенным ПО аппаратных средств или ОС. Подсистема ввода/вывода UEFI может использовать TPM для защищенного хранения определенных метрик, описывающих изменения в конфигурации аппаратных компонентов компьютера, на основе которых принимается решение о целесообразности дальнейшей загрузки системы.

В настоящее время общепризнано, что для гарантированной защиты данных от несанкционированного доступа (НСД) необходимо использовать, принцип пошагового контроля целостности. Данный принцип заключается в выполнении взаимосвязанных последовательных шагов по контролю целостности аппаратных, а затем и программных компонентов компьютерной системы. При этом на раннем этапе активизации компьютера (включение питания, работа базовой подсистемы ввода/вывода) в системе должен присутствовать резидентный компонент безопасности, целостность встроенного ПО которого обеспечивается технологически. Данный модуль позволяет проводить аппаратный контроль целостности на ранних стадиях и, тем самым, обеспечивает неизменность и дальней-

шую активизацию программных средств статического/динамического контроля целостности и разграничения доступа. Таким образом формируются цепочки доверия.

Статическая цепочка доверия SRTM (Static Root of Trust for Measurements) формируется при загрузке системы (рисунок 1), а динамическая цепочка доверия DRTM (Dynamic Root of Trust for Measurements) – во время ее выполнения. Статическая цепочка доверия начинается, когда компьютер включается (или перезагружается), первое измерение выполняется аппаратным обеспечением (то есть процессором) для измерения модуля с цифровой подписью, предоставляемого производителем чипсета. Процессор проверяет подпись и целостность подписанного модуля перед его выполнением. Затем этот модуль измеряет первый модуль кода BIOS/UEFI, который может выполнять следующие измерения. Таким образом, каждый компонент измеряет следующий компонент в цепочке. Пройдя всю цепочку от корня доверия, можно гарантировать неизменность текущего компонента (например, ОС), предоставляющего доверенную среду для более высокоуровневого компонента (например, приложений). Динамическая цепочка доверия формируется с некоторого известного состояния во время загрузки.

Таким образом, доверенная загрузка – это технология, которая обеспечивает цепочку доверия для всех компонентов во время загрузки. Роль ключевого компонента безопасности, обеспечивающего доверие ко всей цепочке загрузки ПО от базового, до прикладных программ, переносит фокус угроз на уязвимости аппаратного уровня и уровня UEFI.

Следует отметить, что существуют и отечественные решения, реализующие концепцию пошагового контроля целостности, которые получили название аппаратных модулей доверенной загрузки (АМДЗ). В отличие от TPM это узкоспециализированные активные аппаратные компоненты, которые принудительно перехватывают загрузку для проведения контрольных процедур. Как правило, АМДЗ входят в состав программно-аппаратных комплексов средств защиты информации от НСД [4].

Восстановление системы

Не смотря на наличие развитых систем контроля и обеспечения целостности и многообразие форм такого контроля, реализующего принцип эшелонированной защиты для повышения устойчивости ОС, в ряде случаев может потребоваться восстановление системы. К наиболее частым причинам, требующим восстановления системы, относятся:

– вирусное заражение, если системные файлы невозможно восстановить или невозможно удалить компоненты вредоносного ПО;

– неверные системные настройки;

– сбои после установки обновлений или стороннего ПО;

– утрата системных файлов;

– невозможность запуска системы.

ОС обладают различными возможностями и степенью автоматизации в зависимости от типа, версии и производителя, но, как минимум, существуют следующие возможности:

– сброс параметров ОС до заводских настроек по умолчанию или переустановка ОС;

– создание полной копии диска для последующего восстановления системного тома.

В первом случае может использоваться созданный в процессе установки диск восстановления или загрузочный установочный диск ОС, а в результате восстановления будет утрачено все установленное ПО и, возможно, пользовательские данные. Во втором случае все данные на диске, как относящиеся к системе, так и приложения, и пользовательские данные будут восстановлены на момент создания образа диска. Однако хранение такого образа может потребовать достаточно большого объема дискового пространства.

Образ носителя информации (всего физического диска или системного раздела) может быть создан с помощью стороннего специализированного ПО, в том числе, и свободно распространяемого, например, AccessData FTK Imager для Windows систем и MacOS, встроенной команды dd или утилит dc3dd, dcfldd для Linux. К этому же типу восстановления можно отнести доступное для некоторых ОС восстановление предыдущего состояния раздела с использованием ранее созданного снимка файловой системы (ZFS для ОС Solaris и Free BSD, BTRFS для Linux). Для создания образа диска, а также восстановления или установки с его использованием, могут использоваться решения резервного копирования и восстановления, такие как Acronis Backup/ True Image, Paragon Backup & Recovery и др.

В Linux среде доступно программное обеспечение с открытым исходным кодом Clonezilla (https://clonezilla.org/), предназначенное для клонирования физических дисков и отдельных разделов, а также создания резервных копий и аварийного восстановления системы. Clonezilla сохраняет и восстанавливает только использованные блоки на жестком диске, что ускоряет процесс создания образа. Доступны три варианта Clonezilla: Clonezilla live, Clonezilla lite server и Clonezilla SE (серверная версия). Clonezilla lite или SE позволяет клонировать множество (более 40) компьютеров одновременно. Поддерживается восстановление одного изображения на несколько локальных устройств. Поскольку речь идет о создании образа дискового пространства, хранение резервной копии может потребовать больших накладных расходов – объем целевого раздела, куда сохраняется копия, должен быть не меньше исходного.

Кроме двух указанных базовых возможностей, доступных практически для любой ОС, могут поддерживаться и другие механизмы восстановления, такие как восстановление из архивного образа системы или точек восстановления.

Серверные версии Windows включают встроенную систему архивации (Windows Server Backup), которая позволяет создавать образы системы и восстанавливать ОС сервера (состояние ОС и данные критических томов) или весь сервер, включая тома с данными, из выбранного архивного образа. При этом можно планировать расписание создания архивных копий и сохранять их локально на отдельном жестком диске или логическом томе, либо в сетевой папке. Создаваемый архивный образ может содержать: файлы и каталоги, тома файловой системы, приложения, состояние системы.

Компания Microsoft предлагает и более развитый инструмент System Center Data Protection Manager (DPM) для резервного копирования и восстановления данных в корпоративной среде. Данные резервных копий при этом могут храниться в пулах дисков, за пределами локальной сети в облаке Microsoft Azure (с использованием службы архивации Azure), на магнитной ленте стримера, которую можно хранить вне помещений организации. DPM позволяет осуществлять следующие виды резервного копирования:

– с поддержкой приложений Microsoft, включая SQL Server, Exchange и SharePoint;

– файлов, а также папок и томов для компьютеров под управлением серверных и клиентских версий ОС Windows;

– состояния системы либо исходного состояния системы для физических компьютеров под управлением серверных или клиентских версий ОС Windows;

– виртуальных машин Hyper-V под управлением Windows или Linux. Можно создать резервную копию всей виртуальной машины или резервные копии с поддержкой приложений Майкрософт на виртуальных машинах Hyper-V под управлением Windows.

Резервное копирование состояния системы включает следующие компоненты.

– член домена: файлы загрузки, база данных регистрации классов COM+, реестр;

– контроллер домена: Active Directory (NTDS), файлы загрузки, база данных регистрации классов COM+, реестр, системный том (SYSVOL);

– службы кластера на компьютерах: дополнительно копируются метаданные кластерного сервера;

– службы сертификатов на компьютерах: дополнительно копируются данные сертификатов.

Резервирование исходного состояния системы создает резервные копии файлов ОС и всех файлов за исключением пользовательских данных на критических томах [1]. Резервная копия исходного состояния системы по определению включает резервную копию состояния системы.

В десктопных версиях ОС Windows доступны следующие средства восстановления [6]:

– восстановление системы (System restore, rstrui.exe) из точки восстановления;

– восстановление файлов из теневых копий;

– восстановление файлов пользователя из архивной копии, созданной с помощью инструмента архивации данных;

– восстановление ОС с помощью образа системы;

– возвращение ОС к первоначальным настройкам с помощью параметров восстановления, диска восстановления или установочного диска;

– удаление установленного обновления.

Восстановление системы – встроенный компонент ОС, который позволяет восстановить работоспособность ОС путем отката до состояния (системных файлов, ключей реестра, установленных приложений), записанного в определенный момент времени, – точке восстановления (restore point). Применение точки восстановления удалит все программы, которые были установлены после ее создания, и не восстановит удаленные раннее файлы. Данные пользователя восстановлением системы не затрагиваются.

Точки восстановления создаются автоматически при возникновении определенных системных событий, например, установка новых приложений или драйверов, а также установка критических обновлений. В случае выполнения операции восстановления также создается точка восстановления, что обеспечивает обратимость операций восстановления системы. Точки восстановления могут также создаваться периодически по заданному расписанию (которое настраивается через Планировщик заданий Task Scheduler), или вручную. Для хранения точек восстановления выделяется определенная часть системного диска, размер которой можно настраивать. По мере заполнения предоставленного им дискового пространства более давние точки восстановления удаляются и на их место сохраняются новые.

Начиная с Windows 7 появилась возможность просмотреть, на какие приложения повлияет откат системы к выбранной точке восстановления. Поиск затрагиваемых программ позволяет определить, какие программы и драйверы придется в случае необходимости переустановить после отката.

Средство восстановления системы, начиная с Windows Vista, базируется на теневом копировании томов (Volume Shadow Copy). Теневые снимки тома представляют собой исходные копии тома, созданные на момент выполнения операции создания точки восстановления. Поэтому, если для логического раздела (даже несистемного) включена защита системы, доступно восстановления предыдущих версий файлов. Предыдущие версии файлов не создаются на дисках с файловой системой FAT и FAT32. Запуск восстановления файлов осуществляется командой «Восстановить прежнюю версию» (Restore previous versions) контекстного меню диска, папки или конкретного файла.

Центр архивации и восстановления Windows включает встроенные утилиты резервного копирования, позволяющие производить как архивирование пользовательский данных на выбранных томах, так и создать образ системы и диск аварийного восстановления.

Образ системы (system image) представляет собой «моментальный снимок» системного раздела, на который установлена ОС Windows, со всеми программами и файлами, присутствующими на нем. Кроме основного раздела Windows, можно включить в создаваемый образ и другие разделы. Утилита создания образа системы работает только с томами NTFS.

Диск восстановления можно использовать для загрузки среды восстановления Windows и получения доступа к набору диагностических и восстановительных утилит. Необходимость в нем может потребоваться в случае утраты или повреждения критических файлов ОС, когда загрузка системы невозможна. Диск аварийного восстановления позволяет восстановить ОС из точки восстановления системы или вернуть компьютер в исходное состояние (к параметрам по умолчанию). Те же варианты восстановления доступны при использовании загрузочного установочного диска.

Возврат ОС к первоначальным настройкам приводит к переустановке Windows, с возможностью сохранить или удалить личные файлы из профиля пользователя. Установленные приложения и драйвера будут удалены. Возврат компьютера в исходное состояние не требует предварительного создания диска восстановления или образа системы и может быть произведено через Панель управления Windows из раздела параметров восстановления системы.

В случае, если нестабильная работа ОС вызвана установкой обновления, недавно установленное обновление системы можно удалить через Центр обновления Windows, используя журнал просмотра обновлений.

ОС Linux не имеет автоматизированных инструментов восстановления наподобие точек восстановления Windows-систем. Алгоритм предпринимаемых для восстановления работоспособности ОС действий зависит от причины возникновения проблем (сбой файловой системы, некорректное обновление дистрибутива, некорректные настройки и прочее). Вместе с тем

существует ряд решений, позволяющих создавать снимки системы наподобие точек восстановления Windows.

TimeShift (https://github.com/teejee2008/timeshift) – инструмент восстановления Linux-системы с графическим интерфейсом. Создает снимки файловой системы с использованием rsync и жестких ссылок или снимков файловой системы BtrFS. Поддерживает создание снимков по заданному расписанию, несколько уровней резервного копирования и фильтры исключений. TimeShift предназначен только для резервирования и восстановления системных файлов, по умолчанию пользовательские данные не включены в снимок. Можно указать чтобы в резервные копии системы входили выбранные данные из домашней папки пользователя. Состояние системы можно восстановить со снимка во время работы системы или при загрузке с Live CD / USB. TimeShift доступен для Debian/Ubuntu/Linux Mint, последние релизы работают в Wayland-сеансах в Fedora и других дистрибутивах.

Systemback (https://sourceforge.net/projects/systemback/) – простая утилита с графическим интерфейсом для создания резервных копий и точек восстановления системы и конфигурационных файлов пользователя. Резервные копии создаются только по желанию пользователя. Доступны некоторые дополнительные возможности, такие как создание Live-образа из существующей установки, установка системы с созданного образа, обновление системы, копирование системы из одного раздела в другой и прочее. Существует возможность восстановить или переустановить загрузчик GRUB 2. Разработка и поддержка Systemback прекращена автором в апреле 2017 года, однако утилита работает в современной версии Linux Ubuntu 18. Для установки Systemback в Ubuntu можно воспользоваться PPA-репозиторием.

Для дистрибутивов Linux на основе RPM доступны централизованные механизмы, реализующие восстановление пакетов (в том числе и относящихся к ядру), то есть откат к предыдущим версиям. Для это используется менеджер пакетов YUM (Yellowdog Updater, Modified). С помощью команды `yum downgrade` можно откатиться к предыдущей версии пакета, а `yum history` позволяет просматривать историю обновлений пакета и отменять отдельные транзакции. Следует отметить, что при откате зависимости пакета не проверяются и не изменяются автоматически, так что их надо обрабатывать отдельно.

Многообразие инструментов контроля, обеспечения и восстановления целостности системных ресурсов, доступных на сегодняшний момент как в ОС семейства Windows, так и для Linux систем, позволяет осуществлять гибкий подбор необходимых средств защиты, исходя из баланса требований безопасности и эффективности работы ОС. Использование и настройка выбранных средств защиты и восстановления должны

тщательно планироваться, и периодичность выполнения контрольных проверок системных ресурсов закрепляться в требованиях политики безопасности.

Список литературы

1. Данные, поддерживаемые для резервного копирования с помощью DPM, 14.03.2019 [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/system-center/dpm/dpm-protection-matrix?view=sc-dpm-2019 (дата обращения: 25.08.2019).
2. Использование средства проверки системных файлов для восстановления отсутствующих или поврежденных системных файлов [Электронный ресурс]. URL: https://support.microsoft.com/ru-ru/help/929833/use-the-system-file-checker-tool-to-repair-missing-or-corrupted-system (дата обращения: 25.08.2019).
3. Используем Secure Boot в Linux на всю катушку, 18.08.2016 [Электронный ресурс]. URL: https://habr.com/ru/post/308032/ (дата обращения: 15.03.2019).
4. Каннер А.М. TPM и IMA/EVM против программно-аппаратных средств защиты информации от НСД [Электронный ресурс]. URL: http://www.okbsapr.ru/kzi_kanneram_2018_1.html (дата обращения: 25.08.2019).
5. Кокорева О. Реестр Windows 7. – СПб.: БХВ-Петербург, 2010. – 704 с.
6. Параметры восстановления в Windows 10 [Электронный ресурс]. URL: https://support.microsoft.com/ru-ru/help/12415/windows-10-recovery-options#section5 (дата обращения: 25.08.2019).
7. Проверка целостности системных файлов Windows 10, 28.11.2018 [Электронный ресурс]. URL: https://remontka.pro/files-integrity-windows-10/ (дата обращения: 25.08.2019).
8. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows. 6-е изд. Часть 1. – СПб.: Питер, 2013. – 800 с.
9. Специальные нормативные документы – ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (дата обращения: 25.08.2019).
10. Extended Verification Module [Электронный ресурс]. URL: https://wiki.gentoo.org/wiki/Extended_Verification_Module (дата обращения: 25.08.2019).
11. GELI(8) // FreeBSD System Manager's Manual [электронный ресурс]. URL: https://www.freebsd.org/cgi/man.cgi?query=geli&sektion=8&manpath=free-bsd-release-ports (дата обращения: 15.03.2019).
12. Integrity Measurement Architecture [Электронный ресурс]. URL: https://wiki.gentoo.org/wiki/Integrity_Measurement_Architecture (дата обращения: 25.08.2019).
13. Integrity Measurement Architecture (IMA) [Электронный ресурс]. URL: https://sourceforge.net/p/linux-ima/wiki/Home/ (дата обращения: 25.08.2019).
14. Juhyung Son, Sungmin Koo, Jongmoo Choi, Seong-je Choi. Quantitative analysis of measurement overhead for integrity verification, April 2017 [Электронный ресурс]. URL: https://www.researchgate.net/publication/317158853_Quantitative_analysis_of_measurement_overhead_for_integrity_verification (дата обращения: 25.08.2019).
15. SDB: Ima evm [Электронный ресурс]. URL: https://en.opensuse.org/SDB:Ima_evm (дата обращения: 25.08.2019).

УДК 004.056

Правовые основания использования средств мониторинга в корпоративной информационной среде

И. Н. Васильева, к.ф.-м.н., доцент,
Г. М. Чернокнижный, к.т.н., доцент,
Санкт-Петербургский Государственный Экономический Университет

В настоящее время в корпоративной информационной среде предприятий широко используются различные средства мониторинга и журналирования [4]. Контроль информационной инфраструктуры используется как для решения задач администрирования, так и для анализа защищенности и обеспечения безопасности корпоративной среды. Вместе с тем, могут возникнуть вопросы юридического обоснования применения таких средств, а также законности использования данных, полученных с их помощью.

Как правило, такие вопросы поднимаются в отношении DLP-систем, позволяющих контролировать действия пользователей на прикладном уровне, включая чтение переписки, удаленное видеонаблюдение, контроль обращений к веб-ресурсам и т.п. Вопрос о законности применения такого контроля в корпоративной среде вызван действиями ст. 23 Конституции РФ, гарантирующую неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. К иным сообщениям могут быть отнесены любые формы электронного взаимодействия – электронные письма, сообщения в закрытых чатах и социальных сетях, мессенджерах, а также файлы, переданные или полученные пользователем по сети. Ограничение этого права допускается только на основании судебного решения.

С другой стороны, предприятие является собственником инфраструктуры и оборудования, применяемого в процессе передачи информации, и имеет право контролировать процесс его использования (в соответствии с ч. 2 ст. 209 ГК РФ). Более того, согласно ст.22 ТК РФ, работодатель обязан обеспечивать работников необходимым оборудованием и иными средствами, необходимыми для исполнения ими трудовых обязанностей.

Это ставит первый вопрос – где проходит грань между правами сотрудника на неприкосновенность частной жизни и тайну переписки, с одной стороны, и выполнением им своих рабочих обязанностей с использованием имущества предприятия, с другой, что подразумевает защиту своих прав работодателем. Ответ на этот вопрос уже более-менее сформирован в юридической среде.

Право работодателя контролировать переписку работника не исключается полностью, однако это право должно быть закреплено в локальном нормативном акте предприятия. В частности, право работодателя на контроль за электронными сообщениями работников, которые отправляются с корпоративных адресов электронной почты, может быть установлено в Правилах внутреннего трудового распорядка организации наряду с обязанностью работника использовать электронную почту только в рабочих целях (ч. 4 ст. 189 ТК РФ). Рекомендуется также указать конкретные цели, в которых работодатель вводит такой контроль [2].

Кроме того, требуется соблюдение условия осведомленности работника об факте осуществления контроля и использования полученных с его помощью сведений. Таким образом, необходимо получение согласия работника на осуществление контроля за его электронной перепиской с корпоративных адресов электронной почты. Например, такое условие может быть включено непосредственно в трудовой договор. Другой вариант – сотрудник должен быть ознакомлен под роспись с локальном нормативным актом, в котором устанавливается право работодателя контролировать корпоративную переписку или осуществлять мониторинг действий сотрудника. Это отвечает требованиям российского трудового права – согласно ст. 22 ТК РФ, работодатель обязан ознакомить работников под роспись с принимаемыми локальными нормативными актами, непосредственно связанными с их трудовой деятельностью.

Все это призвано гарантировать, что сотрудник был предупрежден о возможности осуществления контроля со стороны работодателя, поэтому сотрудник осознает, что он не может рассчитывать на сохранение конфиденциальности переписки с рабочего места. С другой стороны, работодатель получает документальное подтверждение осведомленности сотрудника. Соблюдение этих условий согласуется и с позицией европейского суда по правам человека (ЕСПЧ).

Очевидно, что возможность такого контроля не распространяется на сообщения, отправленные сотрудником с личных устройств (или из дома с личного почтового ящика). Например, ответ на вопрос «Законно ли увольнение работника за распространение коммерческой тайны, если этот факт был установлен при просмотре его личной (не корпоративной) почты?» отрицателен. Если сведения о пересылке информации, содержащей коммерческую тайну, были получены работодателем с нарушением принципов тайны переписки, они будут признаны недопустимыми доказательствами и не смогут подтвердить правомерность увольнения (кассационное определение Судебной коллегии по гражданским делам Волгоградского областного суда от 01.09.11 по делу № 33-11601/11) [2].

Вместе с тем, личные устройства широко используются сотрудниками как для доступа к корпоративным ресурсам, так и для ведения деловой

переписки. Важно, чтобы использование личных устройств было регламентировано политиками информационной безопасности предприятия. Следует, однако, отметить, что с точки зрения трудового законодательства обязательным для исполнения сотрудником являются не политики безопасности, а правила внутреннего трудового распорядка (ст. 21 ТК РФ), которые должны вводить обязательство соблюдения политик. С технической точки зрения, осуществление контроля использования мобильных устройств для работы с корпоративной информацией возможно при организации подключения к корпоративным данным и службам через виртуальную среду с установленным DLP-решением (Virtual DLP) без сохранения данных локально на устройстве [3]. В этом случае работа с данными фактически производится в пределах виртуальной среды, а контроль осуществляется внутри и на границах корпоративной инфраструктуры.

Даже если использование личных устройств разрешено политикой, доступ к внешней сети (Интернет) может быть предоставлен работодателем только в служебных целях, что так же должно быть регламентировано внутренними документами предприятия. Кроме того, предприятием могут выдаваться корпоративные адреса электронной почты или учетные записи других систем обмена сообщениями (например, мессенджеров). С юридической точки зрения возможность контроля работодателем использования таких аккаунтов вызывает гораздо больше вопросов.

Однозначно можно утверждать, что в этом случае при надлежащем юридическом оформлении работодатель вправе осуществлять лишь проверку использования сотрудниками доступа к сети Интернет или служебных аккаунтов в личных целях. С другой стороны, техническая возможность осуществления такого контроля может потребовать получения доступа и к содержимому сообщений. В этой связи интерес представляет постановление ЕСПЧ по делу румынского инженера Богдана Барбулеску, который был уволен после того, как работодатель выяснил, что он использовал служебный аккаунт в мессенджере для ведения личной переписки, что было запрещено правилами компании. ЕСПЧ признал право работодателя «убедиться в том, что сотрудники в рабочее время исполняют свои профессиональные обязанности» и не усмотрел нарушения прав сотрудника, поскольку это можно было сделать только после чтения самой переписки. Суд упомянул также директиву Рабочей группы по защите личных данных от 2002 года, согласно которой работодатель может контролировать рабочую переписку сотрудников, в случае, например, если работник заболел, а вести переговоры с партнерами необходимо. Вместе с тем, данное решение носит прецедентный характер и не означает автоматической возможности чтения переписки сотрудников.

Как правило, при внедрении DLP-системы организация предпринимает следующие действия [1].

1. Сведения о DLP-системе или иной системе мониторинга вносятся в трудовые договоры (или дополнительные соглашения к нему), в правила внутреннего трудового распорядка и другие нормативные документы, регламентирующие деятельность сотрудника в организации (например, должностные инструкции).

Указывается, что все ресурсы, которые используются в работе, являются собственностью работодателя. Владельцем электронной почты и абонентом телефонной сети является организация, таким образом, они предоставляются работнику во временное пользование в период выполнения служебных обязанностей, и их использование в личных целях запрещено. Тогда, если сотрудник пользуется ими в личных целях, он подлежит дисциплинарному взысканию за нецелевое использование рабочих ресурсов или за нарушение правил трудового распорядка.

2. Чтобы сотрудники не могли пожаловаться на нарушение тайны связи, в трудовой договор (или дополнительные соглашения к нему), правила внутреннего распорядка и должностные инструкции вносятся положения о том, что рабочее оборудование и средства коммуникации принадлежат работодателю. Они передаются сотруднику в пользование и предназначены только для выполнения должностных обязанностей, их использование в личных целях запрещается.

Если сотруднику для работы требуется учетная запись в каком-либо мессенджере, то выдача таких учетных записей с паролями должна быть регламентирована, сотрудник должен получать ее под личную ответственность и подтвердить получение ее личной подписью.

3. Разрабатывается регламент мониторинга, в котором должны быть подробно расписаны правила использования, обработки, хранения и передачи конфиденциальной информации внутри организации, а также ответственность, предусмотренная за их нарушения.

Регламент должен содержать пункт о том, каким образом полученные в ходе мониторинга сведения могут быть использованы в дальнейшем, причем заявленная информация должна соответствовать действительности. В случае необходимости проведения аудио и видеозаписи в рамках мониторинга, уведомление об этом также должно быть прописано в регламенте.

4. Все сотрудники компании должны быть ознакомлены с содержанием этого регламента и других организационно-распорядительных документов под роспись.

5. Должны быть приняты необходимые внутренние локальные нормативные акты и разработана организационно-распорядительная документация, определяющие режим коммерческой тайны, режим защиты персональных данных.

6. Разрабатываются правила доступа в Интернет и использования корпоративной информационной инфраструктуры, служебных аккаунтов и

адресов, которые включаются в политики безопасности и инструкции пользователям. Кроме того, в этих документах определяется ответственность за невыполнение этих правил, указывается, что использование корпоративных средств обработки информации контролируется средствами мониторинга. Также должны быть прописаны правила разграничения доступа к защищаемой информации.

Другой вопрос касается грани между получением технической информации об информационной инфраструктуре предприятия и содержимым переписки. Этот вопрос не имеет уже столь однозначного ответа. Сведения о передаваемой внутри корпоративной сети, а также входящей и исходящей информации могут собираться, храниться и анализироваться в целях выявления и блокирования угроз информационной безопасности. Большинство средств защиты информации, а также базовое программное обеспечение (операционные системы) ведут журналы, однако сохраняемая в них информация отражает, как правило, достаточно низкий (технический) уровень организации системы. Как правило, анализ передаваемой информации производится средствами защиты информации в автоматическом режиме. При этом могут обрабатываться как статистические данные о трафике (время, объем передаваемой информации, порты и протоколы подключения, входящие и исходящие IP-адреса, заголовки), так и его содержимое (например, проверка по сигнатурам антивирусной системой или межсетевым экраном).

В то же время некоторые средства защиты позволяют просматривать содержимое захваченного трафика или анализировать подключения на уровне символических имен в ручном режиме, что позволяет уже говорить о существовании принципиальной возможности вмешательства в частную жизнь. Кроме DLP-систем, доступ к содержимому пересылаемой по локальной сети информации может быть получен с помощью снифферов, которые часто используются администраторами сети для обнаружения неполадок, прокси-серверы ведут журналы подключения к внешним ресурсам и т.п. К тому же в последнее время растет число комплексных решений безопасности, совмещающих функциональные возможности различных средств защиты информации.

Юридически провести такую грань достаточно сложно. Гарантом защиты прав человека в этом случае выступает тайна связи, определенная ст. 63 Федерального закона «О связи» от 07.07.2003 №126-ФЗ. Под действие этого закона попадает, например, информация о подключениях к провайдеру, включая IP-адреса абонентов, а также информация об IP-адресах подключений по системам банк-клиент. Данная информация может быть предоставлена, в том числе и представителям правоохранительных органов, только по решению суда. Однако внутри сети предприятия эти ограничения, очевидно, являются абсурдными.

Существуют отдельные попытки разграничения сведений, которые могут или не могут быть отнесены к объекту ст. 23 Конституции РФ, однако системный подход к решению этого вопроса не сформирован. Например, в Постановлении арбитражного апелляционного суда от 19.09.2013 № 09АП-29641/2013, в дальнейшем подтвержденным Определением Высшего Арбитражного суда РФ от 16 июня 2014 г. № ВАС-5501/14, сведения об адресах электронной почты, на которые направлялись электронные сообщения, были исключены из числа сведений, защищаемых ст. 23 Конституции РФ, в связи с тем, что для создания почтового ящика требуется введение логина и пароля, при этом конкретный пользователь – физическое лицо не обязан указывать в адресе электронной почты свои персональные данные, например, Ф.И.О., год рождения и т.п., телефонный номер, паспортные данные. При этом к тайне связи суд с полной определенностью отнес лишь содержание самих электронных сообщений.

В то же время, в постановлении ЕСПЧ от 03.04.07 № 62617/00 по делу Copland v. United Kingdom мониторинг использования электронной почты сотрудника на уровне анализа адресов, дат и времени отправки электронных сообщений был приравнен к контролю переписки [2]. Таким образом, и в этом случае для обеспечения законности контроля со стороны работодателя потребуется соблюдение тех же условий, что и при использовании DLP-систем. Те же соображения можно применить и в случае контроля обращений сотрудников к внешним Интернет-ресурсам.

Это означает, что в разрабатываемых предприятием нормативных документах должны быть предельно четко и конкретно сформулированы области мониторинга (электронная почта, переписка в интернет-мессенджерах, размещение файлов на корпоративных серверах и в системах хранения данных, приложениях коллективного пользования, записи в базах данных, телефонные переговоры и т.п.), его границы и условия, обеспечивающие возможность поддержания эффективного функционирования информационной инфраструктуры предприятия и соблюдение принципа невмешательства в личную жизнь сотрудников и иных лиц.

В регламенте мониторинга рекомендуется также разделять порядок автоматического анализа передаваемой информации техническими средствами (в том числе, содержимого сообщений и файлов) без возможности ознакомления третьих лиц с самой информацией, и порядка ручного контроля содержимого переписки сотрудников с анализом контента.

Список литературы

1. Кандыбович Д.П. Юридические аспекты внедрения DLP-системы, 16.11.2018 [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/solutions/legal-aspects-of-the-implementation-of-dlpsystem (дата обращения: 10.11.2019).

2. Каспаров С. Проверка электронной почты сотрудников. Как контролировать переписку на законных основаниях, 17.05.2013 [Электронный ресурс]. URL: http://ppt.ru/news/117831 (дата обращения: 10.11.2019).
3. Контроль корпоративной почты на мобильных устройствах iOS и Android, 19.03.2019 [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/498398.php (дата обращения: 10.11.2019).
4. Чернокнижный Г.М. Защита сетевых информационных технологий: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2018. – 131 с.

УДК 371.38

Использование деловых игр при обучении бакалавров информационной безопасности

А. С. Верзилова, студент группы ИБ-1601,
Санкт-Петербургский Государственный Экономический Университет

Актуальность интерактивных методов обучения

Построение целостного образа ситуации в сфере информационной безопасности особо важно для студентов данного направления. Абитуриенты выбирают специальность в вузе исходя из интересов довузовского периода, перспективности и востребованности данного направления. В дальнейшем студент испытывает затруднения, сталкиваясь с обширной областью дисциплин и аспектов информационной безопасности. Однако и после обучения бакалавры в реалиях бизнеса не готовы в полной мере соответствовать требованиям, предъявляемым IT-сектором. Отсутствие понимания практических сторон профессии, опыта работы и навыков поведения в конфликтных или критических ситуациях понижает конкурентоспособность вчерашних выпускников.

Основная тенденция в сфере кибербезопасности – конвергенция существующих целей информационной безопасности от противостояния угрозам к созданию систем, обеспечивающих сохранение полномасштабного функционирования информационных систем в условиях постоянно действующих компьютерных атак. Для бакалавров обостряется необходимость подробного изучения механизмов реализации угроз, уязвимостей, тестирования на проникновение и т.д. В силу того, что обучение бакалавров занимает меньше времени, чем образование специалистов, оно должно характеризоваться большей интенсивностью и более быстрым темпам введения в профессиональную деятельность [3].

Объем задач по ИБ настолько велик, что экстенсивным ростом количества подготавливаемых специалистов с ним не справиться. Необходимо

готовить специалистов, способных разрабатывать и применять средства искусственного интеллекта, машинного обучения и роботизации для решения задач обеспечения кибербезопасности.

Таким образом, можно сделать вывод, что в области информационной безопасности востребовано применение практического подхода, целью которого является приведение содержания и результативности образовательных программ в соответствие с современным уровнем технологической инфраструктуры и ожиданиями ведущих работодателей.

Реализация игрового характера противостояния средств защиты и угроз в киберпространстве становится возможным благодаря моделированию с использованием технологий виртуализации и сетевых полигонов. Технологии виртуализации позволяют при относительно небольших затратах создавать адекватные макеты реальных систем и осуществлять моделирование киберпротивоборства.

В литературе вводится понятие испытательного полигона (киберполигона). Полигон кибербезопасности представляет из себя единый комплекс, в который интегрируются виртуальные учебные лаборатории и другие учебные полигоны. Такое средство реализации практических методов обучения служит площадкой, на базе которой студенты имеют возможность разработать и испытать ноу-хау, проекты, разрабатываемые в рамках НИР практики [3].

Современные образовательные технологии отличаются высокой динамикой развития и методы обучения модифицируются исходя из особенностей сегодняшнего студента: клиповое мышление, заинтересованность в геймификации процесса познания, постановка «больших» задач, поиск своего места в ряду специалистов и самоутверждение в выбранной области.

Сфера образования характеризуется появлением актуальных интерактивных форматов.

В методических рекомендациях Российской правовой академии министерства юстиции Российской Федерации под интерактивным обучением понимается специальная форма организации познавательной деятельности, для которой характерно осуществление совместной деятельности студентов, при которой все участники взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации, оценивают действия других и свое собственное поведение, погружаются в реальную атмосферу делового сотрудничества по разрешению проблемы.

Место деловых игр в системе активных методов обучения представляется возможным определить исходя из существующих классификаций образовательных технологий. В современной педагогике среди подходов в области интерактивных методов выделяют следующие:

– творческие задания;

– обучающие игры (ролевые игры, имитации, деловые игры);

– использование общественных ресурсов (приглашение специалиста, экскурсии);

– социальные проекты и другие внеаудиторные методы обучения (соревнования, интервью, фильмы, спектакли, выставки);

– изучение и закрепление нового материала (интерактивная лекция, работа с наглядными пособиями, видео- и аудиоматериалами, «обучающийся в роли преподавателя», «каждый учит каждого», мозаика (ажурная пила), использование вопросов, сократический диалог);

– тестирование;

– обсуждение сложных и дискуссионных вопросов и проблем (займи позицию, шкала мнений, ПОПС-формула);

– разрешение проблем («дерево решений», «мозговой штурм», «анализ казусов», «лестницы и змейки»);

– тренинги [1].

Таким образом, деловая игра является частью общей системы интерактивных методов обучения и отличается от других обучающих игр.

Специфика деловых игр

Деловая игра как метод имитации разнообразных условий профессиональной деятельности (включая экстремальные) и принятия решений при наличии конфликтных ситуаций или информационной неопределенности позволяет бакалаврам самых разных профилей перейти в практическую плоскость во время образовательного процесса.

Проблематика проведения деловых игр в условиях современного образования заключается в том, что в литературе нет четкого понимания и регламентации деловых игр как метода обучения. На практике также под деловыми играми понимают другие ответвления обучающих игр или вовсе иные образовательные технологии.

Для формулировки более четкого определения деловой игры целесообразно выделить признаки, отличающие этот метод обучения. В настоящее время выделяют следующие признаки деловых игр:

1. Наличие проблемы управления социально-экономической или социально-психологической системой.

2. Наличие общих целей всего игрового коллектива.

3. Наличие различных ролей и в соответствии с ними различие интересов (конфликт) участников.

4. Невозможность полной формализации системы, наличие неопределенности в обстановке, учет вероятностного характера многих факторов и, исходя из этого, наличие игровой имитационной модели рассматриваемого процесса.

5. Наличие реального или условного фактора времени.

6. Динамичность изменения обстановки и наличие обратной связи, зависящей от решений участников игры в предыдущие моменты времени и влияющей на изменение обстановки в последующие.

7. Наличие системы оценки результатов игровой деятельности.

8. Наличие системы мотивации участников, дающей объективную оценку личного вклада каждого участника игры в достижение общей цели, общего результата деятельности игрового коллектива.

9. Многоальтернативность решений.

10.Обязательное минимально необходимое и достаточное документальное обеспечение.

11.Наличие управляемого эмоционального напряжения [2].

Исходя из вышеперечисленных признаков можно составить полное представление о феномене деловых игр.

Деловая игра позволяет значительно сократить время накопления профессионального опыта, дает поле для экспериментов с различными подходами и стратегиями решения сложившейся ситуации. Такой вид обучения позволяет формировать у будущих профессионалов целостное представление области, с которой им придется столкнуться в бизнес-среде.

Игра обладает особой практической ценностью, поскольку снимает противоречия между абстрактным характером учебного предмета (объекта) и реальным характером профессиональной деятельности, способствует введению участников в динамику развития сюжета деловой игры, формированию целостного образа профессиональной ситуации. Результативность деловых игр подтверждается следующими сведениями: прочитанное запоминается на 10%; услышанное – на 20%; увиденное – на 30%; увиденное и услышанное одновременно – на 50%; осуществленное действие – на 90%

Обзор деловых игр в области информационной безопасности

Пример блиц-игры. Компания ищет сотрудника на вакансию.

Задачи участников игры:

– для кандидатов: доказать, что Вы лучший кандидат на объявленную вакансию;

– для представителей компании: разработать критерии оценки кандидатов и выбрать лучшего претендента;

Критерии оценивания результатов: наиболее полные и приближенные к реальности критерии кандидатов, лучшая презентация кандидата исходя из выбора представителей компании [2].

Деловая игра направлена на подготовку будущих бакалавров к собеседованиям, усвоения навыка самопрезентации и выступления перед публикой, развивает коммуникативные навыки. Данное мероприятие ставит также целью научить студентов компетентно и беспристрастно оценивать

участников рабочего процесса, обосновывать свою точку зрения и анализировать необходимые профессиональные компетенции.

Регламентом определяется время на подготовку: 30 минут.

Пример мини-кейса. Работа осуществляется в группах, каждая из которых представляет собой экспертную комиссию по расследованию инцидента.

Описание ситуации: В 7:30 утра в крупную компанию на КПП человек принес чертежи, которые имеют эмблему компании и метку ДСП. Человек, который принес документы, утверждает, что нашел их на тротуаре только что и решил принести в организацию. Дан список лиц, допущенных до работы с данной документацией, с краткой характеристикой. Пример базируется на прецедентах судебной практики.

Задание: каждая команда должна разработать последовательность действий расследования инцидента и представить одну наиболее вероятную версию происходящего.

Критерии оценивания: наиболее обоснованная позиция, самая полная и соответствующая действительности стратегия расследования, приближенность к реальному событию согласно судебной практике.

Игра рассчитана на 1 академический час.

Деловая игра направлена на развитие критического мышления, улучшение навыков информационно-аналитической деятельности, усвоение процесса делопроизводства и организации режима защиты информации на предприятии. Кроме того, студенты в процессе игры улучшают навык работы в команде и обоснования своей профессиональной точки зрения.

Пример игры с дополнительным оборудованием. Перед командой игроков несколько ПК, принтер, wi-fi-адаптер, Bluetooth-адаптер, коммутатор [4]. Все устройства находятся в неисправном состоянии. Выдается журнал для протоколирования действий команды, назначается главный администратор и секретарь.

Задача команды: привести все устройства в рабочее состояние и провести базовую настройку (создать учетные записи пользователей и администратора с различными правами доступа, настроить сетевую печать, создать локальную сеть и пр.).

Критерии оценивания: приближенность к запрашиваемому результату, число устройств, находящихся в рабочем состоянии по завершении работы, полнота отчета и т.д.

Деловая игра направлена на отработку практических навыков, дает поле для отработки креативных идей и способов работы, развивает навык работы в команде. Такая деловая игра направлена на проверку базовых знаний студентов по работе с программно-техническим обеспечением, ПК и периферией, позволяет почувствовать себя в роли системного администратора.

Список литературы

1. Безматерных Т.А. Управление внедрением в учебный процесс инновационных методов, форм и средств обучения – Ростов-на-Дону: Российская правовая академия министерства юстиции Российской Федерации, 2014 [Электронный ресурс]. URL: https://rostov.rpa-mu.ru/Media/rostov/Svedenia_ob_OO/Obrazovanie/metodicheskie_rekomendacii/interaktiv.pdf (дата обращения: 10.11.2019).
2. Зарукина Е.В. Деловые игры: история, теория, практика обучения – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2014 [Электронный ресурс]. – URL: https://docplayer.ru/28436011-Delovye-igry-istoriya-teoriya-praktika-e-v-zarukina-direktor-centra-innovacionnyh-obrazovatelnyh-tehnologiy-k-e-n-docent.html (дата обращения 13.11.2019).
3. Зегжда Д.П. Специалист по кибербезопасности. Что ждет работодатель? – Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого, 2019.
4. Чернокнижный Г.М. Лабораторные практикумы по сетевым дисциплинам информационной безопасности // Информационное противодействие угрозам терроризма – Том: 1 – № 25 – Таганрог, 2015. – С. 403-408.

УДК 004.056

Критерии выбора DLP-систем

И. Г. Гниденко, к.э.н., доцент,
И. В. Егорова, к.э.н., доцент,
Санкт-Петербургский Государственный Экономический Университет

В условиях формирования цифровой экономики резко возрастает ценность информации как для отдельного гражданина, компании, так и государства в целом. Огромный объем информации хранится сейчас в банковской и телекоммуникационной сферах, медицинских и государственных учреждениях. Количество таких данных увеличивается, возможности их анализа очень быстро совершенствуются, поэтому резко возрастает необходимость защиты данных от потенциальных злоумышленников.

Несмотря на постоянное совершенствование методов противодействия утечкам, обеспечить абсолютную защищенность чувствительных данных чрезвычайно сложно. Таким образом, системы защиты от утечек данных (DLP – Data Leak Protection) сегодня не только не теряют своей актуальности, но и становятся все более востребованными в организациях и на предприятиях самого разного профиля.

Рынок зарубежных DLP-систем достаточно обширен. Например, в обзоре компании «Gartner» за 2019 год дан рейтинг 16 таких систем [2].

В настоящее время основными игроками мирового рынка DLP-систем являются компании, которые широко известны другими своими продуктами для обеспечения информационной безопасности в организациях. Это, прежде всего, Symantec, McAffee, TrendMicro, WebSense. Общий объем мирового рынка DLP-решений оценивается в 400 млн долларов, что совсем немного по сравнению с тем же рынком антивирусов [2].

По прогнозу Gartner, к 2022 г. 60% предприятий будут вовлекать в разработку стратегии в области предотвращения утечек информации не только специалистов по информационной безопасности (ИБ), но и руководителей бизнес-подразделений, тогда как сейчас этот показатель составляет только 15%. Кроме того, к 2020 г. 85% организаций внедрят хотя бы одно интегрированное решение DLP, в то время как сейчас таковое имеет только половина компаний. В то же время, согласно прогнозу, к 2020 г. именно на долю интегрированных продуктов будет приходиться основная доля дохода от продаж DLP [3].

В России интерес к DLP-системам начал возникать в связи с громкими инцидентами, связанными с утечками информации и работой законодательных органов в области защиты информации. Начало развития рынка DLP-систем относится к 2000 годам, хотя и до этого времени существовали специальные приложения, обеспечивающие защиту конфиденциальных данных организации от утечек.

Первыми в России внутренними угрозами подобного уровня заинтересовалась «Лаборатория Касперского» и уже через два года компания выделила под разработку DLP-системы собственную дочернюю систему. Так появилась компания InfoWatch, которую можно считать первопроходцами в этой области. Однако эксперты самой компании делали очень скромные прогнозы по развитию данной отрасли. Прибыль флагманский продукт начал приносить лишь в 2012, но уже после этого доход ежегодно вырастал на 60-70%.

Последние исследования SearchInform, ведущего игрока на российском рынке информационной безопасности, показали, что сейчас в России и странах СНГ DLP-системы не пользуются большой популярностью. Только чуть более половины организаций (58%) планируют в скором времени установку комплексной защиты. Остальные не считают нужным ее внедрение либо полагают, что достаточно и частичной защиты. Однако, информационная безопасность только тогда будет на оптимальном уровне, когда обеспечена комплексная защита [4].

Наиболее популярные и широко распространенные на данный момент в России DLP-системы перечислены в таблице 1.

В настоящее время рынок DLP-систем растет достаточно быстро. Разработчики предлагают разнообразные решения на любой вкус и кошелек. Для того, чтобы выбрать оптимальную систему для своего бизнеса нужно, хотя бы в общих чертах, знать принципы работы DLP-систем.

Таблица 1 – Российские DLP-системы [6]

№	Название системы	Фирма-производитель
1.	Гарда Предприятие	(ООО «Гарда Технологии», бывш. ООО «МФИ Софт»
2.	Solar Dozor	ООО «Солар Секьюрити», входит в структуру ПАО «Ростелеком»
3.	InfoWatch Traffic Monitor Enterprise	АО «ИнфоВотч»
4.	Falcongaze SecureTower	ООО «Фалконгейз
5.	Контур информационной безопасности	ООО «Сёрчинформ»
6.	Zecurion Zgate 4.0, Zlock 5.0, Zdiscovery 2.0	АО «СекьюрИТ»

Функционирование DLP-систем базируется на особом алгоритме работы удаленного агента с главным программным комплексом, который представляют собой «ядро» из связки служб и подсистем, которые вместе отвечают за обнаружение и категоризацию информации, нуждающейся в защите от утечек. Основных технологий, которые применяются в большинстве DLP-решений две: лингвистический анализ и использование статистических методов. Так же могут присутствовать технологии распространения меток или формальные методы анализа. Лингвистический метод анализа включает в себя:

– морфологический анализ – поиск по всем возможным словоформам информации, которую необходимо защитить от утечки;

– семантический анализ – поиск по вхождению важной информации в содержимом файла.

Статистические методы анализа включает в себя несколько этапов работы с документами:

– на первом этапе документ (текст) делится на фрагменты приемлемой длины (чтобы обеспечить точность срабатывания). С фрагментов снимается хеш (в DLP-системах иногда встречается термин Digital Fingerprint – «цифровой отпечаток»);

– на втором этапе хеш сравнивается с хешем фрагмента, взятого из документа. При совпадении система помечает документ как конфиденциальный и действует в соответствии с политиками безопасности.

Функционал DLP-систем необходимо рассматривать с нескольких сторон. Первая сторона, которую стоит рассмотреть – режимы работы. В зависимости от топологии защищаемой сети, DLP-системы могут работать в трех режимах, названных по условному принципу действия: «копия», «в разрыв» и «комбинированный». Режим «копия» применяется в сетях, в которых блокировать нежелательный трафик не представляется

возможным, например, из-за отсутствия определенных компонентов, нужных для блокировки. Например, из-за отсутствия подконтрольных DLP-системе коммутаторов. В этом случае, утечка информации произойдет, однако, система будет иметь копию документа, конфиденциальность которого была нарушена, а также данные нарушителя и устройства, с которого произошла утечка. При наличии необходимых технических ресурсов, система способна работать в режиме «в разрыв». Данный режим позволяет производить блокировку действия, которое могло бы привести к утечке информации за безопасный периметр компании. Комбинированный режим работы предполагает совместное использование двух ранее упомянутых режимов. Стоит отметить, что при работе режима «в разрыв» системой предусмотрена работа службы, которая, в случае ложного срабатывания, способна повторно отправить документ по месту назначения. Таким образом, отправителю не нужно повторять отправку информации, а получатель может не беспокоиться о том, что информация до него не дойдет.

Вторая сторона – контролируемые каналы информации. Современные DLP-системы способны контролировать все наиболее популярные каналы передачи информации. В списках контролируемых каналов присутствуют такие как:

– почтовые SMTP, IMAP4, POP3 и др.;
– интернет HTTP(S), FTP(S);
– съемные носители;
– мессенджеры ICQ, Skype, Jabber и др.;
– локальные и сетевые принтеры;
– сетевые хранилища, локальные диски рабочих станций;
– мобильные устройства, включая почту, SMS, мессенджеры, камеру и т.д.

И последняя, третья сторона – выведение отчетности. Здесь у разработчиков DLP-систем гораздо больше свободы в возможности реализации данного функционала. Стандартно необходимая отчетность представляет собой информацию о действиях, которые были совершены пользователем или на отдельной рабочей станции. Таким образом, можно более подробно изучить каждого работника на наличие в его рабочем процессе нарушений и оценить общую эффективность. В этом вопросе некоторые системы предоставляют специалисту по безопасности большую информацию, чем другие. Это обусловлено тем, что функционал в данной области может быть развит вплоть до автоматического формирования профиля каждого работника с собранной подробной статистикой вплоть до распределения по времени каждого действия наблюдаемого сотрудника. Специалист по безопас-

ности и руководство, которым предоставлен доступ к консоли оператора DLP-системы, могут изучить данный вид информации и предпринять необходимые действия согласно правилам компании [1].

При выборе DLP-системы нужно учитывать специфику данного класса программных продуктов. К особенностям выбора DLP-системы относятся следующие:

– скорость обработки данных;
– предотвращение утечек информации по максимальному числу каналов;
– возможность мониторинга работы агентов;
– учет особенностей установки и последующей поддержки системы;
– удобство работы с системой.

Что касается критериев сравнения DLP-систем, то различные авторы [3, 6-8] предлагают целый ряд параметров при выборе системы, таких, как:

– целевая аудитория;
– наличие сертификатов;
– типы лицензий;
– тип технической поддержки;
– доступные языки интерфейса;
– производительность;
– возможности блокировки;
– предоставляемые отчеты;
– работа с политиками безопасности;
– использование СУБД;
– экспертиза, опыт и надежность разработчика;
– наличие, качество и быстрота реакции техподдержки;
– цена и стоимость владения системой, и т.д.

Однако, к главным критериям выбора DLP-системы большинство авторов относит:

1. минимальные (рекомендуемые) системные требования;
2. каналы передачи информации, контролируемые DLP-продуктом;
3. механизмы контроля пользователей;
4. технологии и методы анализа данных;
5. возможности интеграции.

Достаточно важный критерий при выборе DLP-системы – это цена. В этой связи следует помнить, что затраты на DLP-систему включают не только стоимость самого продукта. Окончательная сумма формируется по нескольким статьям расходов. К ним относятся: стоимость лицензий, стоимость внедрения, количество специалистов, необходимых для обслуживания системы, стоимость техподдержки, стоимость обновлений.

Также хочется отметить, что решения класса DLP – это не коробочные продукты, для их полноценного внедрения и запуска в промышленную эксплуатацию требуется интеграция в ИТ-инфраструктуру компании, тонкая настройка компонентов, разработка перечня политик, долгая борьба с ложными срабатываниями и преодоление других специфических препятствий.

Что касается предложений компаний к разработчикам, то они, в основном, относятся к повышению производительности, улучшению интерфейса, расширению технологических возможностей.

К перспективам развития DLP – решений можно отнести внедрение новых средств и методов машинного обучения, использование технологии Big Data (в связи с ростом объема собираемых данных), улучшение алгоритмов поиска и распознавания (в том числе, голоса).

Список литературы

1. Гниденко И.Г., Егорова И.В., Дубских Н.А. Современные dlp-системы. Опыт практического использования// Инновационные технологии в науке и образовании. Сборник статей XII Международной научно-практической конференции. Пенза, 2019 – Изд-во «Наука и просвещение» – С. 36-41.
2. Reviews for Enterprise Data Loss Prevention [Электронны ресурс]. URL: https://www.gartner.com/reviews/market/enterprise-data-loss-prevention/vendors (дата обращения: 10.11.2019).
3. SearchInform. DLP-системы [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/ (дата обращения: 10.11.2019).
4. В «магическом квадранте» Gartner по DLP-решениям появился третий российский вендор, 22.02.2017 // IT Research. Аналитика российского рынка ИТ [Электронный ресурс]. URL: https://www.itbestsellers.ru/products/detail.php?ID=37170 (дата обращения: 10.11.2019).
5. Защита корпоративных данных с помощью DLP-системы [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/ (дата обращения: 10.11.2019).
6. Степанов И. Сравнительный обзор средств предотвращения утечек данных (DLP), 2019 [Электронный ресурс]. URL: https://safe-surf.ru/specialists/article/5233/609990/ (дата обращения: 10.11.2019).
7. Петручев Н. Обзор популярных российских DLP-систем, 2019. [Электронный ресурс]. URL: https://vc.ru/services/75433-obzor-populyarnyh-rossiyskih-dlp-sistem (дата обращения: 10.11.2019).
8. Гридасов В. Импортозамещение DLP-систем в России, 2017 [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/ Options_import_substitution_DLP_systems_Choose_migration_options (дата обращения: 10.11.2019).

УДК 371.38

Обоснование критериев перевода системы обучения инженерных кадров в автоматизированную среду подготовки

А. А. Горшков, адъюнкт,
ВУНЦ ВМФ «Военно-морская академия»,
Д. Ю. Федоров, старший преподаватель,
Санкт-Петербургский Государственный Экономический Университет,
А. Ю. Астахов, оператор научной роты,
О. А. Зиангиров, оператор научной роты,
ВУНЦ ВМФ «Военно-морская академия»
В. А. Зимин, к.т.н., доцент,
Военно-морской политехнический институт
ВУНЦ ВМФ «Военно-морская академия»

Деятельность современных инженеров подразумевает под собой наличие сложной системы научных и профессиональных знаний, умений и навыков, личностных и профессиональных способностей. На фоне общего развития мира в условиях быстро изменяющейся информационной среды и роста достижений научно-технического прогресса происходит значительное усложнение задач, возникающих в инженерной практике, которые требуют новых подходов как непосредственно в подготовке инженеров, так и в управлении процессом их обучения.

Повышение эффективности и качества инженерного образования можно достичь:

- увеличением общего срока обучения;
- интенсификации образовательного процесса;
- углублением и расширением подготовки инженеров;
- комплексной рационализацией образовательного процесса.

При этом необходимо помнить, что при увеличении времени на усвоение и переработку информации, сообщаемой обучающимся, нужно учитывать различные уровни познавательных возможностей человека, в частности, способности к скорости восприятия и переработки информации. Также необходимо учитывать два основных правила усвоения информации в процессе обучения [1]:

– за любой располагаемый промежуток времени можно добиться либо усвоения обучаемым большого количества информации, но на более низком уровне усвоения; либо меньшего количества информации, но на более высоком уровне усвоения;

– вместе с ростом информации при постоянном сроке обучения возможно либо снижения уровня усвоения, либо тщательный отбор и обобщение информации при условии сохранения заданного уровня.

В любом случае здесь надо понимать, что можно идти либо вширь, либо вглубь при одном и том же содержании подготовки инженеров, при неизменном времени их обучения, но нельзя достичь того и другого одновременно (рисунок 1) [1].

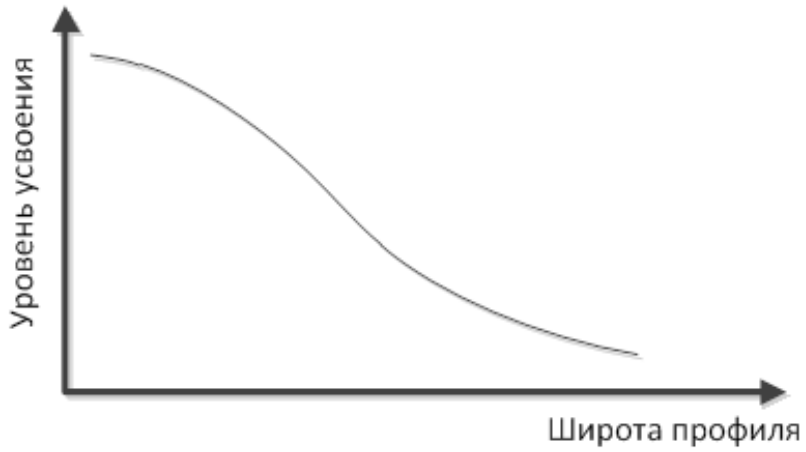

Рисунок 1 – Соотношение широты профиля подготовки обучающихся и уровня усвоения учебного материала

Комплексная рационализация образовательного процесса по подготовке специалистов предполагает создание научно обоснованных последовательности и согласованности преподавания отдельных учебных дисциплин с целью сокращения времени на их изучение и за счет этого включение в программы новых тем и разделов. Основой содержания дисциплин должны являться не знания преподавательского состава, а модель эффективной инженерной деятельности выпускников с учетом перспектив ее развития.

Современный этап развития образовательных технологий характеризуется широким внедрением информационно-вычислительных средств поддержки образовательного процесса. Это позволяет повысить качество и эффективность процесса обучения за счет интенсивного использования различных программно-аппаратных средств подготовки. Поэтому, по мнению авторов, для повышения эффективности подготовки инженерных кадров необходимо частично управление процессом обучения передать автоматизированной среде с использованием новых информационных технологи.

Проблема перевода системы подготовки инженерных кадров в автоматизированную среду может быть сформулирована как кибернетическая педагогическая задача по управлению процессом обучения. Реализация принципов кибернетической педагогики получила развитие в программированном (программном) обучении.

Программируемое обучение – это дидактическая система, возникшая в результате проникновения идей кибернетики в педагогику, которая исходит из психолого-педагогических закономерностей и требований оптимизации управления процессом обучения [3].

Процесс обучения, исходя из концепции программированного обучения, представляет собой строго расчлененный во времени процесс. Это расчленение на так называемые элементарные акты обучения, соответствующие элементарным «порциям» учебной информации, должно производиться не на основе так называемого педагогического опыта, а на основании объективных критериев (логико-математической оценки и пр.), обеспечивающих оптимальность такого разбиения.

Руководящий тезис программированного обучения состоит не в утверждении единственности такого «наилучшего» разбиения, а в признании принципиальной возможности произвести разбиение с точки зрения некоторой фиксированной совокупности выбранных критериев и возможности найти такие объективные (в точно оговоренном смысле) критерии.

Перевод процесса управления обучением в автоматизированную среду, на взгляд авторов, *должен* обеспечить непрерывность процесса подготовки инженерных кадров. Требование непрерывности является принципиальным для результативности перевода системы подготовки в автоматизированную среду [2].

Неразрывность среды подготовки обеспечивается эффективными междисциплинарными связями. Установление подобных связей возможно только при условии реальной структуризации педагогических знаний, составляющих суть учебных дисциплин программ профессиональной подготовки инженерных кадров. Основная причина того, что система педагогических знаний системы подготовки специалистов слабо структурирована, заключается в трудностях формализованного представления этих знаний. Решив принципиально эту проблему, можно выйти на создание сквозной интегрированной системы обучения специалистов и единой базы инженерных знаний предметной области, как содержательной основы процесса обучения в автоматизированной среде подготовки, или как сейчас принято называть в единое электронное образовательное пространство.

Областью формализации знаний занимается такое направление искусственного интеллекта, как инженерия знаний и данных [4]. От правильного выбора способа представления знаний зависит ход разработки системы, а также удобство ее сопровождения. Интеллектуальные модели представления знаний, которые необходимы для управления процессом обучения, объективно должны обладать двумя принципиальными свойствами: иметь широкие описательные возможности и свойство оцениваемости [6].

До настоящего времени специалистами по искусственному интеллекту предложен целый ряд моделей представления знаний: правила, семантические сети, фреймы, сценарии, логика, концептуальные схемы и др., а также их сочетания. Каждая модель имеет свои преимущества и недостатки, сравнительный анализ которых произведен в работе [5, 6].

Для процессов управления обучение инженеров лучше всего подходят языково-алгебраические формальные методы, так как они обладают одновременно свойствами достаточно широкого описания и оценивания. Наибольший интерес, по мнению авторов, для данных целей представляют собой семантические сети. Они имитируют естественное понимание и использование человеческого языка, обладают большими описательными возможностями, наглядностью форм представления знаний. Это обусловило их широкое распространение в практике моделирования представления знаний, особенно при создании систем гибридного интеллекта.

Особо стоит отметить применение семантических сетей знаний (сети знаний), предложенные профессором В.Я. Розенбергом на базе математической «Теории исчисления знаний» [7]. В своей теории он рассматривает то, что все множество знаний является системой, состоящей из взаимосвязанных элементов, которыми являются понятия, определяющие смысл объектов, их свойств и процессов в заданной предметной области. Содержание каждой предметной области представлено конечным числом понятий. В системе понятий можно выделить те, которые находятся в основании (понятия нижнего уровня), затем понятия, которые опираются на понятия нижнего уровня и т.д. Таким образом, систему знаний можно представить в виде иерархического направленного графа – семантической сети знаний. Вершинами данного графа являются термины, обозначающие понятия изучаемой предметной области. Связи в графе образуются за счет включенности одних терминов в определения других терминов. Благодаря этому, процесс обучения, возможно, представить как перемещение по направленному графу, то есть сети знаний, например, курса подготовки специалиста (рисунок 2).

Развитие теории профессора Розенберга В.Я. имеет место в работах [2, 8], в которых предлагается кибернетический подход к управлению процессом обучения на основе формализации знаний с применением семантических сетей знаний, что представляет большой интерес для их дальнейшего исследования.

Непрерывность, четкая структуризация и упорядоченность педагогических знаний позволит развить такой критерий автоматизированной среды обучения как **адаптивность.** Адаптивная автоматизированная система обучения должна приспосабливаться к уровням обученности обучающегося (обучающихся), как количественным, так и качественным. Это, безусловно, является важным условием при организации управления

процесса обучения. Примеры моделей адаптивной автоматизированной системы обучения на основе использования семантических сетей представлены в работах [9, 10].

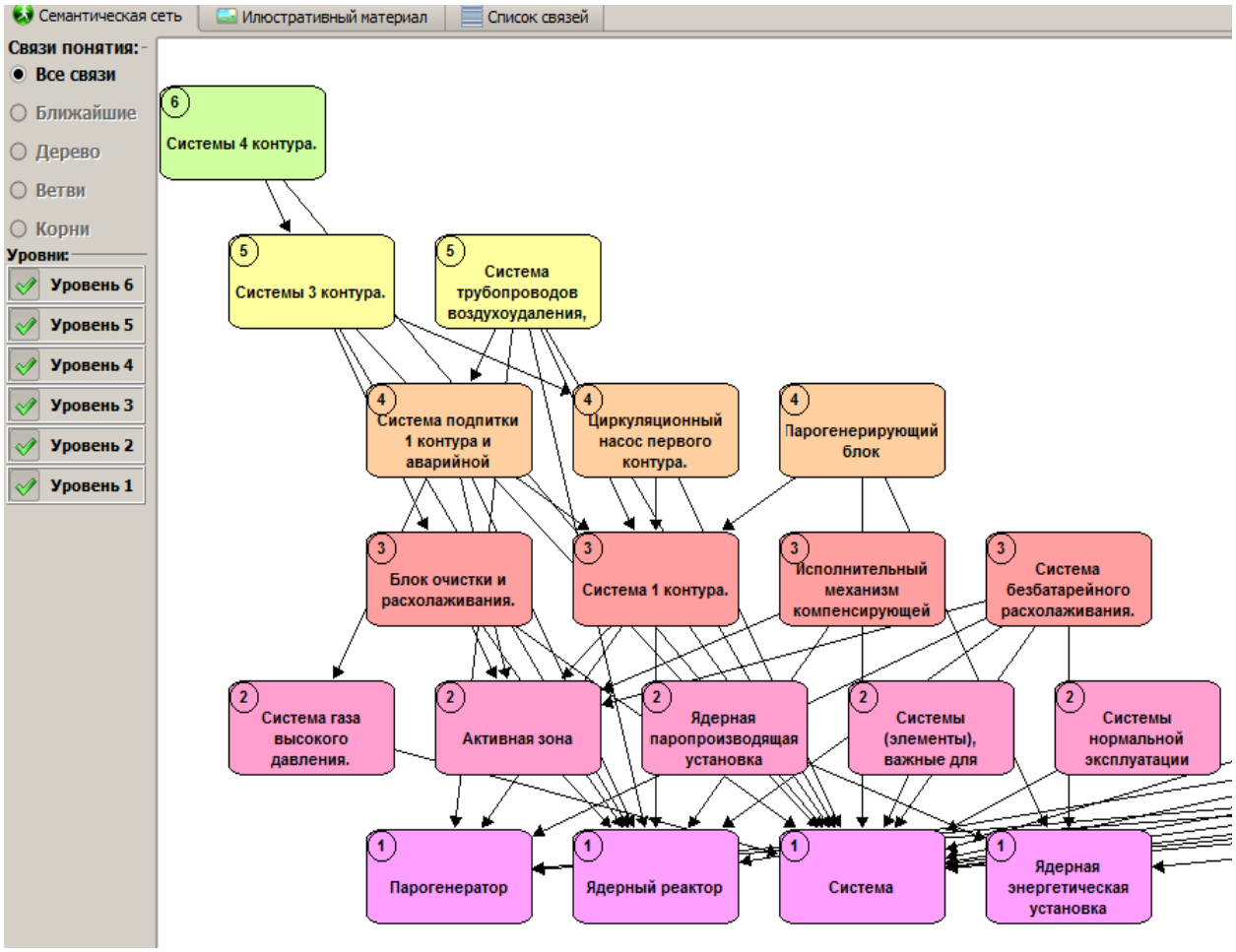

Рисунок 2 – Фрагмент сети знаний

Непрерывность процесса обучения, структуризация педагогических знаний с их адекватной формализацией представления, а также адаптивность автоматизированной системы подготовки являются необходимыми и достаточными критериями перевода процесса управления обучение в автоматизированную среду.

Использование семантических сетей знаний является наиболее мощным и универсальным средством моделирования и оценки для широкого класса автоматизированных систем обучения, позволяющих в единых формализмах учесть специфические особенности деятельности инженеров в автоматизированной среде подготовке.

Перевод системы обучения инженерных кадров в автоматизированную среду подготовки позволит повысить эффективность управления процессом обучения и обеспечит согласованность всех этапов обучения за счет:

− наглядного представления содержания всего курса подготовки инженеров в виде упорядоченной многоуровневой непрерывной сети;

− установления четких взаимосвязей между дисциплинами;

− оперативной корректировки объема учебных программ дисциплин, с учетом их взаимосвязей, необходимости и возможности изменений их содержания, необходимого времени обучения;

− установление взаимосвязей между различными уровнями образования и инженерной подготовки специалистов;

− адаптации автоматизированной среды обучения уровню обученности как к отельного обучающегося, так и к целой группы.

Список литературы

1. Жаркой Э.Ф. Технология обучения. – СПб.: ВВМИОЛУ им. Ф.Э. Дзержинского, 1994. – 153 с.
2. Волынец Ю.Ф. Теоретические основы построения и сущность процесса обучения в автоматизированной среде подготовки специалистов ВМФ. [Текст]: дис. док. пед. наук: 20.02.02: утв. 28.07.00 – Петродворец, 2000. – 208 с. – Библиогр.: с. 286-308.
3. Александров Г.Н., Ратнер Г.Л. Программированное обучение и его место в медицинских вузах. – М.: Медицина, 1968. – 184 с.
4. Гаврилова Т.А., Кудрявцев Д.В., Муромцев Д.И. Инженерия знаний. Модели и методы: Учебник. – СПб.: Издательство «Лань», 2016. – 324 с.
5. Актуальные проблемы инфотелекоммуникаций в науке и образовании. 5 Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т. 2/ под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевич, 2016. – 432 с.
6. Кобзев В.В., Шилов К.Ю. Методы создания технических средств обучения корабельных операторов. – СПб.: Наука, 2005. – 156с.
7. Розенберг В.Я. Знания – основа безопасности (основы математической теории исчисления знаний) // Национальная безопасность и стратегическое планирование, 2015. – № 1(9). – С. 26-34.
8. Федоров Д.Ю. Кибернетический подход к управлению процессом обучения на основе семантических сетей знаний. – СПб.: Изд-во Политехн. ун-та, 2016. – 40 с.
9. Бобыр Е.И. Комплексная модель адаптивной компьютеризированной системы обучения и тестирования на базе семантических сетей/ Е. И. Бобыр, Л. Н. Радванская, В. В Мартынов, Ю. В. Чепурная // Вестник Херсонского национального технического университета. – 2009. – № 1 (34). – С. 491-496.
10. Сметюх Н.П. Разработка адаптивной компьютеризированной системы обучения специалистов водного транспорта в процессе промысла // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. – 2016. – №3(37). – С. 217-227.

УДК 004.71

Состояние и перспективы развития производителей коммутационного оборудования Cisco и D-Link

Б. И. Зарипов, студент группы ИБ-1601,
О. С. Лямзин, студент группы ИБ-1601,
Санкт-Петербургский Государственный Экономический Университет

Коммутатор – это один из видов сетевых устройств, с его помощью можно соединить несколько сетевых узлов (ПК, телефоны или другие сетевые устройства). При этом соединение не будет выходить за рамки одного или нескольких сегментов сети [1].

Анализируя информацию о деятельности компаний, производящих коммутационное оборудование, за 2009 год, можно сделать вывод о том, что лидирующую позицию по числу продаж в мире занимала компания Cisco (США), а второе место – D-Link (Тайвань).

На рисунке 1 представлены графики распределения долей рынка между компаниями в сегменте коммутаторов на начало 2009 года по результатам исследования, проведенного аналитической компанией In-Stat [2]. Однако, к 2019 году D-Link не входит даже в топ 5 компаний, продающих коммутационное оборудование.

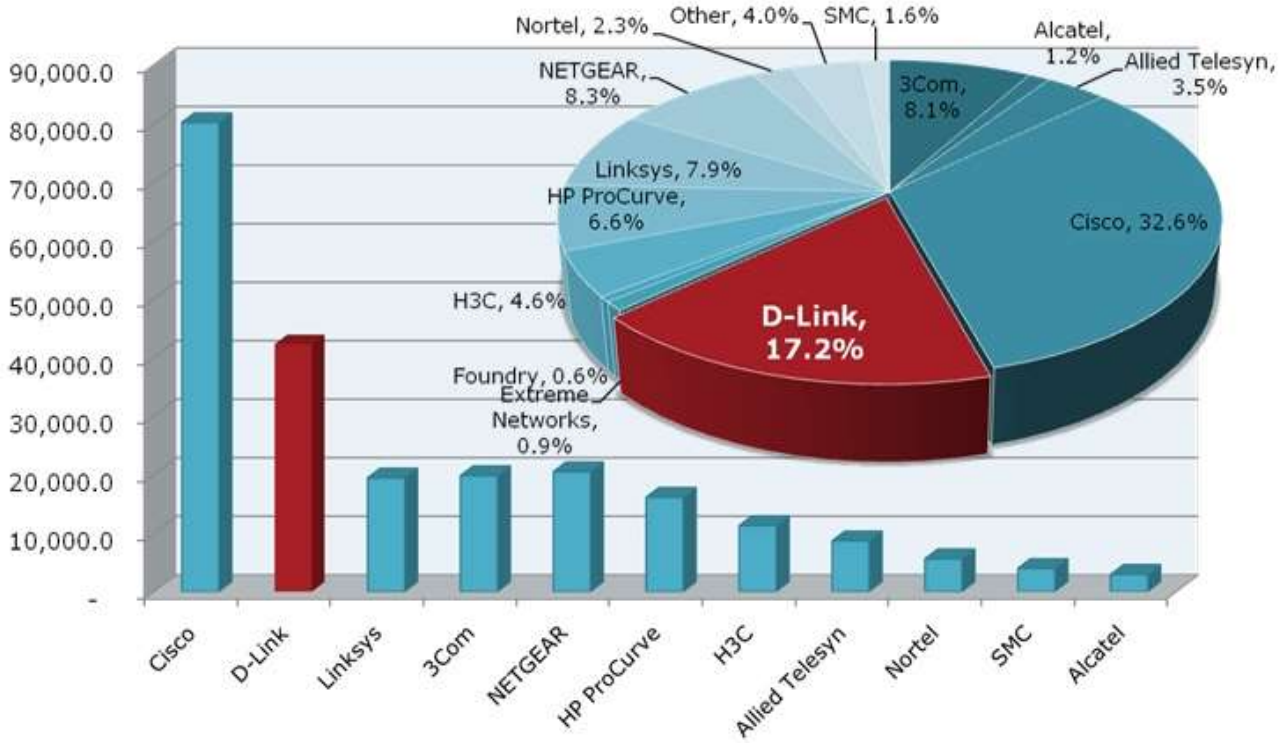

Рисунок 1 – Распределение рынка коммутаторов на начало 2009 года [2]

На рисунке 2 представлен график распределения долей рынка между компаниями в сегменте коммутаторов на середину 2019 года по результатам исследования, проведенного компанией IDC [3].

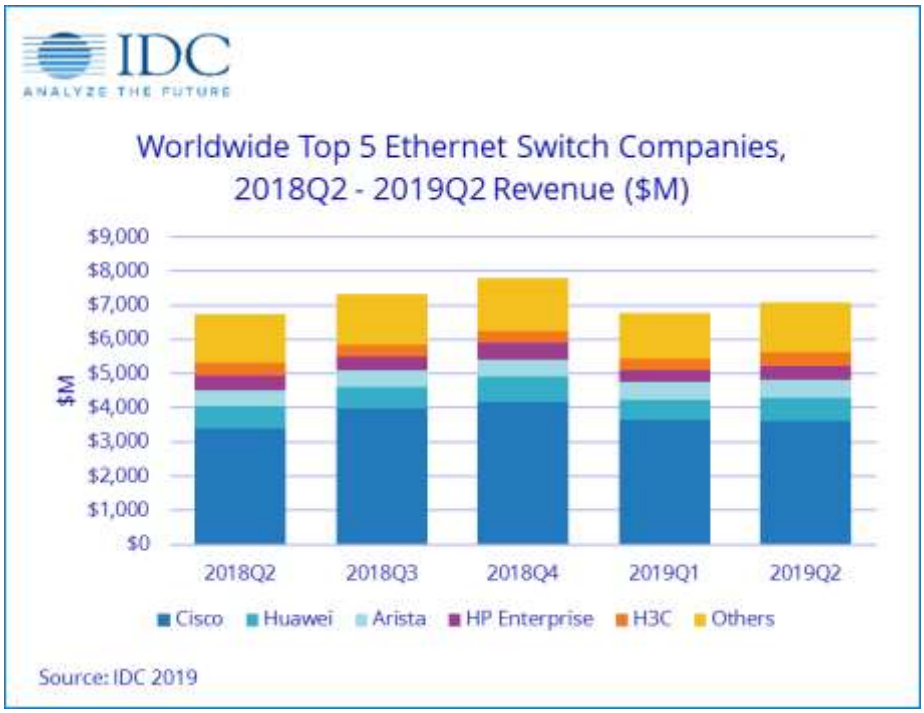

Рисунок 2 – Распределение рынка коммутаторов в 2019 году [3]

Также об отрицательной динамике D-Link свидетельствует падение стоимости ее акций за последние 5 лет. Компания Cisco, в свою очередь, характеризуется положительной динамикой цен на акции, что отражено на рисунке 3 [4, 5].

Рисунок 3 – Динамика изменения стоимости акций компаний D-Link и Cisco [4, 5]

Цены устройств, производимых компаниями, разительно отличаются. Так, например, при сравнении коммутаторов D-link DGS-1210-26/F и Cisco WS-C2960S-24TS-S, имеющих практически одинаковые технические характеристики, можно сделать вывод о том, что коммутатор компании Cisco дороже коммутатора D-Link почти в четыре раза. Сравнение коммутаторов представлено в таблице 1.

Таблица 1 – Сравнение коммутаторов Cisco и D-Link

Характеристика	Коммутатор D-link DGS-1210-26/F [6]	Коммутатор Cisco WS-C2960S-24TS-S [7]
Количество портов	24	24
Базовая скорость передачи данных	10/100/1000 Мбит/сек	10/100/1000 Мбит/сек
Количество uplink/стек/sfp-портов и модулей	2	2
Максимальная скорость uplink/sfp-портов	10/100/1000 Мбит/сек	10/100/1000 Мбит/сек
Внутренняя пропускная способность	52 Гбит/сек	50 Гбит/сек
Размер таблицы mac адресов	8192	8196
Объем флэш-памяти	32 МБ	64 МБ
Объем оперативной памяти	128 МБ	128 МБ
Цена	от 7 603 ₽	от 28 900 ₽

Не смотря на политику цен, лидирующее положение Cisco на рынке обеспечивается: отказоустойчивостью, гибкостью настройки, совместимостью продуктов между собой, возможностью поиска неисправностей, собственными инновационными технологиями.

Все устройства D-Link работают на ядре Linux, и это дает возможность изменять программное обеспечение. У Cisco своя операционная система для оборудования – IOS, но изменение работы аппаратной части устройств не предусмотрено.

Компания Cisco создает и выкладывает в открытый доступ образовательные программы, связанные с освоением оборудования Cisco [8].

Аналогичную программу обучения предоставляет пользователям компания D-Link. Доступ к курсам обучения компания D-Link предоставляет авторизированным пользователям [9].

Главное отличие обучающих программ компаний в том, что компания D-Link предоставляет 6 курсов обучения, а компании Cisco 36 курсов.

На данный момент компания Cisco реализует несколько направлений развития [10]:

– технологические инновации в области сетей хранения данных [11];
– сотрудничество с крупными компаниями России и мира;

– разработка решений построения сетевой ИТ-инфраструктуры различным платформам;

– организация и проведение конференций, олимпиад, курсов и конкурсов в области сетевых технологий.

Отчет Cisco 2020 Global Networking Trends Report показывает намерения Cisco работать в области искусственного интеллекта [12].

На данный момент компания D-Link реализует несколько направлений развития [13]:

– расширение ассортимента оборудования и программного обеспечения. В течении 2019 года, компания D-Link представила 15 новых продуктов. В их числе различные маршрутизаторы, коммутаторы и программное обеспечение собственной разработки.;

– технологические инновации в области беспроводных сетей.

Проанализировав динамику изменения распределения коммутационного оборудования за 2009-2019 года, можно сделать вывод, что компания Cisco занимает лидирующую позицию на рынке в сегменте коммутаторов, D-link в последние годы потерял позиции. Оборудование компании Cisco дорогое, но имеет высокую гибкость настройки, что позволяет расширить функционал сети, не используя дополнительного оборудования, и отказоустойчивость по сравнению с оборудованием D-Link.

Cisco сотрудничает с большим количеством компаний и развивается в области искусственного интеллекта, а D-Link разрабатывает новые решения для домашних локальных сетей и малых предприятий и постоянно обновляет свою базу продуктов.

Оборудование D-Link предназначено для личного пользования или для компаний небольшого размера, которые ограничены в ресурсах. Оборудование Cisco предназначено в основном для крупных организаций и телекоммуникационных предприятий.

Список литературы

1. Коммутатор: обзор устройства для построения локальной сети [Электронный ресурс]. URL: https://besprovodnik.ru/kommutator/ (дата обращения: 14.11.2019).
2. D-LINK укрепляет позиции на рынке коммутаторов [Электронный ресурс]. URL: http://www.discom.net.ru/news/ proizv_detail.php?ID=555834 (дата обращения 14.11.2019).
3. IDC Trackers Show Moderate Growth in Worldwide Ethernet Switch and Router Markets in Q2 2019 [Электронный ресурс]. URL: https://www.idc.com/getdoc.jsp?containerId=prUS45487019 (дата обращения 14.11.2019).
4. Cisco Systems Inc (CSCO) [Электронный ресурс]. URL: https://ru.investing.com/equities/cisco-sys-inc-chart (дата обращения 14.11.2019).
5. D Link India Ltd (DLIL) [Электронный ресурс]. URL: https://ru.investing.com/equities/d-link-india-ltd (дата обращения 14.11.2019).

6. Коммутатор D-link DGS-1210-26/F [Электронный ресурс]. URL: https://market.yandex.ru/product--kommutator-d-link-dgs-1210-26-f/39608559/spec?track=tab (дата обращения 14.11.2019).
7. Коммутатор Cisco WS-C2960S-24TS-S [Электронный ресурс]. URL: https://market.yandex.ru/product--kommutator-cisco-ws-c2960s-24ts-s/6332739/spec?track=tab (дата обращения 14.11.2019).
8. Список авторизованных курсов Cisco по уровням [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/training/ list_of_cisco_authorized_courses_web.pdf (дата обращения 14.11.2019).
9. D-Link. Категории курсов [Электронный ресурс]. URL: https://learn.dlink.ru/ (дата обращения 14.11.2019)
10. Cisco. Новости [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/about/press.html (дата обращения 14.11.2019)
11. Cisco представляет технологические инновации в области сетей хранения данных [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/about/press/press-releases/2019/09-16.html (дата обращения 14.11.2019).
12. Исследования Cisco показывают готовность ИТ к внедрению искусственного интеллекта и интенционно-ориентированных сетей [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/about/press/ press-releases/2019/11-08.html (дата обращения 14.11.2019).
13. D-Link. Новости [Электронный ресурс]. URL: http://www.dlink.ru/ru/news/ (дата обращения 14.11.2019).

УДК 006.065

Особенности руководства по качеству подразделения по защите информации предприятия малого бизнеса

Д. А. Ильина, студент группы ИБ-1601,
Санкт-Петербургский государственный экономический университет,
А. В. Солодянников, к.т.н., доцент,
Санкт-Петербургский государственный экономический университет,
генеральный директор ООО «Ассоциация специалистов по безопасности»

Наличие и состояние нормативно-методической базы в организации оказывает непосредственное влияние на эффективность функционирования системы менеджмента качества (СМК), системы менеджмента информационной безопасности и системы защиты информации. «Руководство по качеству» является основным документом СМК. В связи с этим разработка «Руководства по качеству» является важной составляющей частью построения системы эффективного менеджмента организации.

Организации составляют, документируют и применяют Руководства по качеству для решения следующих задач:

– знакомство сотрудников с политикой компании в области качества;

– создание документированной базы;

– сохранение действенности и требований системы, особенно в меняющихся условиях;

– уменьшение сроков обучения персонала требованиям системы качества, особенно при частой смене кадров;

– соответствие стандартам ИСО 9001, 9002 [2,3];

– изложение в руководстве не только желания организации удовлетворить потребности потребителя, но также работа, которая предшествует этому.

Руководство по качеству может быть:

– базовым сборником документированных операций системы качества и подобных документов;

– объединением документов системы качества, если есть не только одно руководство;

– последовательностью документированных операций для специального применения;

– сборником нескольких документов или уровней;

– отдельным документом;

– чем-то другим в отличии от вышеперечисленного из-за каких-то различных организационных потребностей.

Проблематика эксплуатации руководства по качеству заключается в том, что в литературе и на практике не существует определенных единых правил о том, как именно нужно его создавать. Некоторые требования прописаны в ГОСТ Р ИСО/ТО 10013-2007.

– Руководство по качеству должно содержать область применения системы менеджмента качества, обоснование и детали любых исключений, документированные процедуры или ссылки на них, описание взаимодействия процессов системы менеджмента качества.

– Руководство по качеству должно включать в себя информацию об организации, в том числе ее наименование, адрес и контактную информацию. В руководстве по качеству может быть приведена дополнительная информация, например, направление деятельности организации, сведения о ее размере, историческая справка.

– Руководство по качеству должно содержать элементы, предусмотренные пунктами 4.4.2-4.4.9, но не обязательно в указанном порядке» [1].

Более детальное описание требований можно представить следующим образом.

– Наименование и область распространения руководства по качеству должны четко определять предприятие, к которому применяется руководство. Этот пункт должен также определять применение требований системы менеджмента качества.

– В содержании Руководства по качеству должны быть указаны порядковые номера и наименования разделов (при необходимости подразделов), приложений с указанием их обозначения и заголовков, а также номера страниц, но которых они помещены.

– Руководство по качеству должно включать в себя политику и цели в области качества или ссылки на них. Решение о включении политики и/или целей в области качества в руководство по качеству принимает высшее руководство организации. Показатели результативности выполнения целей могут быть включены в другие документы системы менеджмента качества организации. Политика в области качества должна содержать обязательства соответствия установленным требованиям и постоянного повышения результативности системы менеджмента качества [1].

– Руководство должно содержать точные сведения о его статусе, датах рассмотрения, утверждения и пересмотра.

– Должен быть список документов, на которые ссылаются в руководстве.

– В руководстве по качеству должна быть описана структура организации. Можно использовать схемы, картинки процессов.

– В руководстве по качеству нужно описывать систему менеджмента качества и ее применение в организации. Рекомендуется указывать методы, которыми выполняется политика и цели в области качества.

При описании требований системы менеджмента качества нужно использовать следующую типовую структуру документации (рисунок 1).

Рисунок 1 – Типовая структура документации системы менеджмента качества

Единого подхода к разработке и использованию «Руководства по качеству» на данный момент не существует. Задача предприятий и организаций – сформировать «Руководство по качеству» таким образом, чтобы данный основополагающий документ регламентировал множество документов и оптимизировал деятельность компании с точки зрения повышения эффективности.

Список литературы

1. ГОСТ Р ИСО/ТО 10013-2007 Менеджмент организации. Руководство по документированию системы менеджмента качества.
2. ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования.
3. ГОСТ Р 57189-2016/ISO/TS 9002:2016 Системы менеджмента качества. Руководство по применению ИСО 9001:2015.

УДК 004.056

Вопросы правового регулирования безопасности Интернета вещей

В. В. Кухарь, студент группы ИБ-1601,
А. А. Никифоров, студент группы ИБ-1601,
Санкт-Петербургский Государственный Экономический Университет

В современном мире термин «Интернет вещей» (Internet of Things, IoT) достаточно популярен. Однако несмотря на его большую распространенность, одного универсального определения у данного термина нет.

В качестве примера более или менее конкретных определений можно привести рекомендации Международного союза электросвязи, которые содержат одно из таких определений и говорят о том, что Интернет вещей – это «глобальная инфраструктура для информационного общества, обеспечивающая современные услуги путем присоединения (физического и виртуального) вещей на основе существующих и развивающихся, функционально совместимых информационно-коммуникационных технологий» [3]. Схожее определение предлагается в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы – интернет вещей в ней определен как «концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека» [2].

Таким образом, термин «Интернет вещей» применим для иллюстрирования этапа развития информационного общества, в котором достаточно

объемная часть взаимодействия в сети осуществляется не между пользователями, а между устройствами. Конечно, с юридической точки зрения взаимодействие должно происходить между конкретными субъектами права, но с технической точки зрения взаимодействуют именно устройство, и как правило, автоматическим образом.

По мнению консалтингового подразделения американской корпорации Cisco IBSG (Internet Business Solutions Group), Интернет вещей – это этап развития информационного обества, когда количество «вещей» или материальных объектов (IoT-устройств), подключенных к Интернету, превысило число людей, пользующихся сетью. Согласно исследование Cisco IBSG, Интернет вещей начал свое существование между 2008 и 2009 г., потому что именно тогда на одного человека стало приходиться более одного подключенного устройства. Прогноз Cisco IBSG таков, что к 2020 г. количество таких объектов возрастет до 50 миллиардов [4].

Интернет вещей обладает огромным потенциалом, но в то же время он сталкивается с рядом барьеров, которые могут помешать его полноценному развитию. В наши дни все чаще появляются постоянные новости об атаках на устройства, подключенные к Интернету, а также новости, касающиеся проблемы в отношении персональных данных и частной. Технические проблемы продолжают оставаться нерешенными, а также возникают новые трудности в области политики, законодательства и дальнейшего развития.

Уже несколько лет высказываются различные точки зрения относительно необходимых правовых изменений в связи с выходом России на путь, предусмотренный Стратегией развития информационного общества в Российской Федерации на 2017-2030 годы, в которой, в частности, Интернет вещей называют одним из ключевых научно-технологических направлений.

Следует отметить, что внутригосударственные правовые изменения осуществляются более неторопливыми темпами по сравнению с активно развивающимися технологиями, и поэтому действия законодательных органов выглядит несколько неактуальными по отношению к происходящему в современном мире. В связи с этим, на данный момент времени правовое регулирование эксплуатации Интернета вещей, а также разработки IoT-устройств регламентирует соблюдение минимальных требований для обеспечения надлежащего уровня безопасности.

В России более широко представлены законодательные ограничения, регулирующие так называемый индустриальный Интернет вещей. В этой области следует отметить Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», вступивший в силу с начала 2018 года [1]. Его можно оценить как важный шаг на

пути к созданию единой согласованной законодательной базы, регламентирующей использование новой технологии. Из названия понятно, что данный закон направлен на регулирование ситуаций, которые могут произойти вследствие несанкционированных действий злоумышленников, направленных на критические важные объекты инфраструктуры.

Однако в сфере бытовых IoT-устройств защита информации пока недостаточно сильна. Это усугубляется тем, что производители зачастую сами способствуют злоумышленникам, изготавливая устройства без каких-либо средств защиты. В результате такие устройства пополняют ряды очередного ботнета или работают на благо киберпреступников каким-либо другим образом. Например, производители дешевых камер практически игнорируют снабжение своих продуктов функциями обеспечения безопасности, поскольку, по их мнению, для большинства пользователей низкая стоимость камер гораздо важнее защищенности.

Исходя из вышесказанного, становится ясно, что термин «Интернет вещей» охватывает собой предметные области, которые имеют между собой мало общего (энергетика, транспорт, промышленность, здравоохранение, торговля, госуслуги, частная жизнь и др.). Таким образом, не может быть одинаковых подходов к регулированию безопасности различных категорий IoT-устройств на всем их жизненном цикле, начиная от разработки продуктов и заканчивая их обслуживанием и эксплуатацией.

На данный момент можно выделить несколько юридически значимых особенностей Интернета вещей, которые являются проблемными и, несомненно, должны быть отражены в законодательстве.

1. В условиях развития «умных» устройств происходит резкое увеличение объема и содержания обрабатываемой ими информации. Такая информация может содержать в себе сведения о реальных субъектах, то есть она перестает иметь чисто техническое значение, и, таким образом, граница между технической информацией и персональными данными стирается. Это связано с тем, что данные, собираемые IoT-устройствами, могут содержать исчерпывающую информацию об отдельных лицах, и эти данные могут использоваться как во благо, например, для разработки функционала, полезного для пользователей, так и во вред, в том числе дискриминирующим образом [5]. В целом, возникают ряд сомнений, например, касательно того, что в условиях Интернета вещей можно соблюсти принципы обработки персональных данных на основе конкретных и заранее определенных целей, а также далеко не всегда возможно получение согласия субъекта персональных данных. Подобное использование IoT-данных приводит к возникновению многочисленных проблем практического, юридического и нормативного характера.

2. IoT-устройства используют Интернет для связи, а Интернет охватывает территории всех государств на всех уровнях. IoT-устройства могут

собирать данные о физических лицах из одной юрисдикции и передавать эти данные для хранения и обработки в другую юрисдикцию, и при этом часто наблюдается нехватка или отсутствие технических барьеров. Это явление может быстро перерасти в юридическую проблему (например, если собранные данные были признаны персональными или конфиденциальными). Устройства способны автоматически подключаться к другим устройствам и системам и передавать данные в другие страны без ведома пользователей. Это способно привести к появлению таких ситуаций, когда пользователь фактически несет юридическую ответственность за соблюдение требований по транснациональной передаче данных, даже не зная, что это происходит. Эти проблемы сложны, но они становятся еще более сложными по мере того, как технологии опережают в своем развитии законодательство.

3. Вещи в формате Интернета вещей выполняют не только свои основные функции, но и начинают накапливать огромное количество внешней информации: дата, время, местоположение, температура воздуха и так далее, и, соответственно, это усиливает проблему объемов оборота информации. Поводом для беспокойства служит несовершенство законодательства о сохранении и уничтожении данных, а также возможность получения доступа к этим данным злоумышленниками.

4. Цикл взаимодействия в сети может быть уже не только анонимным, но и, более того, он может быть автоматическим. То есть правоотношения могут реализовываться с формальной юридической точки зрения, по сути, уже без участия самого человека от начала и до конца. Так как устройства способны автоматически подключаться к другим устройствам и системам, то они могут реализовать достаточно много правоотношений с юридической точки зрения. При этом пользователь может вообще не знать о конкретных деталях, связанных с этими правоотношениями. Это усложняет решение вопросов об ответственности и причинении убытков и вреда такими устройствами.

5. Распространение Интернета вещей влечет очевидно новые риски информационной безопасности, связанные с недобросовестной и неправомерной деятельностью различного масштаба, предполагающей несанкционированный доступ к устройствам, изменение алгоритмов их работы или сбор конфиденциальной информации субъектов Интернета вещей. Часто функция автоматического обновления, а соответственно и устранения существующих уязвимостей программного обеспечения в IoT-устройствах не предусмотрена, однако наличие функции автоматического обновления подразумевает возможность удаленного управления устройством, в том числе, неавторизованным лицом, что может привести к серьезным последствиям. В этой связи возникает общая проблема качества устройств и связанных с ними услуг и вопросы ответственности их производителей за нее. Также в

этом случае информационная безопасность начинает соприкасаться с областью физической безопасности, потому что, например, взлом беспилотного автомобиля и получение доступа к его управлению — это уже не просто информационное нарушение, это уже и угроза жизни и здоровью непосредственно с источником повышенной опасности.

6. Ответственность в связи с использованием устройств Интернета вещей. Один из основополагающих вопросов звучит так: если человеку нанесен вред в результате действия или бездействия IoT-устройства, кто должен нести за это ответственность? На этот вопрос бывает трудно ответить, и во многих случаях мы сталкиваемся с отсутствием законов, которые бы регулировали этот вопрос. Работа IoT-устройств сложнее, чем работа простых автономных продуктов, а это говорит о более сложных сценариях привлечения к ответственности.

7. С распространением популярности устройств, подключенных к Интернету вещей, постепенно сформировывается новый рынок ограниченных ресурсов, например, радиочастотного спектра используемого для функционирования Интернета вещей.

8. Совместимость – также достаточно актуальный вопрос, ведь различные устройства должны быть совместимы между собой для того, чтобы сформировать единую техническую систему. Отсутствие надежного взаимодействия в том числе негативно влияет на безопасность.

На основании рассмотренных выше вопросов, можно сделать вывод о том, что повсеместное распространение Интернета вещей модифицирует и усиливает уже существующие проблемы современного общества, а также создает новые. Особенно актуальны сейчас проблемы правового режима информации, обработки персональных данных и неприкосновенности частной жизни, а также проблемы автоматизированности действий и обеспечения информационной безопасности.

Таким образом, ряд проблем юридического, нормативного и правового характера, связанных с Интернетом вещей, довольно значителен. Развитие IoT-устройств приводит к появлению новых юридических и нормативных проблем, которых раньше не существовало, и усугубляют многие существующие проблемы. По опыту уже организованных атак, четко видно, что безопасность Интернета вещей требует действий как со стороны производителей, так и со стороны государственных органов.

Список литературы

1. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс].URL: http://www.consultant.ru/ document/cons_doc_LAW_220885/ (дата обращения 13.11.2019).

2. Указ Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]. URL: https://base.garant.ru/71670570/ (дата обращения 13.11.2019).
3. ITUT Y.2060 (06/2012) Overview of the Internet of things [Электронный ресурс]. URL: http://www.itu.inl/itut/recommendations/ rec.aspx?rec=Y.2060/ (дата обращения 13.11.2019)
4. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything// Cisco IBSG. April 2011 [Электронный ресурс]. URL: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (дата обращения 13.11.2019).
5. The Internet of Things: an overview. Understanding the Issues and Challenges of a More Connected World// Internet Society. October 2016 [Электронный ресурс]. URL: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (дата обращения 13.11.2019).

УДК 004.056

Обеспечение информационной безопасности при гибком подходе разработки программного продукта

Е. В. Майорова, к.т.н.,
С. А. Соколовская, к.э.н., доцент,
Санкт-Петербургский государственный экономический университет,
А. В. Черток,
главный специалист отдела защиты цифровых продуктов ООО «ИТСК»

В настоящее время разработка и внедрение программного обеспечения (ПО) для нужд бизнеса является одним из важнейших направлений информационных технологий (ИТ). В этом аспекте актуальность приобретают и вопросы информационной безопасности (ИБ). От грамотного построения и использования системы защиты информации при разработке ПО зависит не только финансовое положение, но и репутация Компании, а также соблюдение законодательства РФ.

В рамках действующей Доктрины информационной безопасности [1] прописаны организационные основы ИБ, в том числе и к разработке ПО.

Также в указе Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» определяются «цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой эконо-

мики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов» [2].

Развивая отрасль информационных технологий и электронной промышленности в РФ, делается упор на совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения ИБ [2].

Для разработки ПО в настоящее время используются следующие методологии.

Каскадная:

– последовательное прохождение всех этапов создания ПО;

– следующий этап разработки ПО начинается при условии окончания предыдущего.

Итеративная:

– выполнение работ идет параллельно с непрерывным анализом полученных результатов и корректировкой предыдущих этапов работы;

– прохождение повторяющихся циклов Деминга-Шухарта.

Гибкая:

– взаимодействие всех членов команды и заказчика при создании ПО на каждом этапе;

– быстрое принятие решения и минимизация рисков разработки.

Рассмотрим подробнее гибкую методологию разработки ПО (Agile). В основу этой методологии положен «Манифест гибкой методологии разработки программного обеспечения» [3], основу которого составляют следующий идеи:

1. Взаимодействие людей важнее процессов и инструментов.

2. Хорошо отлаженная система важнее сопровождающей документации.

3. Взаимодействие с заказчиками стоит во главе условий контракта.

4. Готовность к изменениям важнее следования первоначальному техническому заданию.

Основу манифеста [3] составляют 12 принципов, направленных на создание качественного ПО с удобным интерфейсом, а также ориентированных на постоянную связь команды разработчиков друг с другом и с заказчиком в рамках проекта.

Принципы Agile-методологии согласно Манифесту [3]:

– удовлетворение клиента за счет ранней и бесперебойной поставки ценного ПО;

– приветствие изменения требований, даже в конце разработки (это может повысить конкурентоспособность полученного продукта);

– частая поставка рабочего ПО (каждый месяц или неделю, или еще чаще);

– тесное, ежедневное общение заказчика с разработчиками на протяжении всего проекта;

– участие в проекте мотивированных разработчиков, которые обеспечиваются нужными условиями работы и поддержкой;

– рекомендуемый метод передачи информации – личный разговор (лицом к лицу);

– работающее ПО – лучший измеритель прогресса;

– спонсоры, разработчики и пользователи должны иметь возможность поддерживать постоянный темп на неопределенный срок;

– постоянное внимание на улучшение технического мастерства и удобный дизайн;

– простота – искусство НЕ делать лишней работы;

– лучшие архитектура, требования и дизайн получаются у самоорганизованной команды;

– постоянная (частая) адаптация (улучшение эффективности работы) к изменяющимся обстоятельствам.

Преимущественно гибкие методологии направлены на уменьшение рисков методом сведения разработки к сериям непродолжительных циклов – итераций. «Итерация сама по себе выглядит как программный проект в миниатюре и включает все задачи, необходимые для выдачи мини-прироста по функциональности: планирование, анализ требований, проектирование, кодирование, тестирование и документирование» [3, 4]. Обычно отдельная итерация не может служить гарантией выпуска новой версии продукта, но предполагает, что сам проект можно использовать в конце каждой итерации. По завершению каждой итерации команда проводит пересмотр приоритетов разработки.

Следует отметить, что основой гибкой методологии служит рабочий продукт. Отдавая предпочтение непосредственному общению разработчиков и заказчиков, agile-методы уменьшают объем письменной документации, по сравнению с другими методами.

Преимущества использования гибкой методологии:

– быстрое выявление неправильных подходов;

– быстрое принятие решений;

– сотрудничество дает множество преимуществ;

– изменение неизбежная составляющая проекта;

– конечный продукт содержит наиболее полезные функции;

– наиболее привлекательная среда разработки для нового поколения;

– бизнес-группа удовлетворена результатом проекта;

– получение качественного продукта;

– составление технической документации занимает меньше времени и содержит меньше ошибок;

– более простое обслуживание приложения.

На основе методологии гибкой разработки ПО как результат агрегации всех возможных решений и проблем внутри информационно-технических отделов появился гибкий подход к разработке ПО – DevOps (development (Dev), operations (Ops)) [5]. Суть которого заключается в непрерывности интеграции нового функционала и непрерывности поставки этого функционала на продуктивную среду в работающем стабильном состоянии. Следует отметить, что использование безопасности в DevOps требует новых подходов, процессов и инструментов. Вопросы безопасности ПО легче решить с использованием DevSecOps (development (Dev), security (Sec), operations (Ops)) – цикл разработки программного обеспечения, в котором особое внимание уделяется безопасности.

Преимущества DevSecOps основаны на автоматизации процессов [5]:

– позволяет снизить вероятность неправильного администрирования и ошибок, которые часто приводят к простоям или открывают поверхность для атак;

– избавляет ИБ-специалистов от необходимости настраивать консоли вручную;

– активирует программно все функции безопасности, работу брандмауэров и сканирование уязвимостей.

В результате такого подхода команды, занимающиеся безопасностью, могут сосредоточиться на установке политик безопасности [5].

При разработке ПП в рамках подхода DevSecOps определим основные подготовительные работы по внедрению процессов ИБ:

1) сформировать набор функциональных требований к разрабатываемой системе в виде пользовательских историй;

2) разработать дизайн и архитектуру проекта;

3) с точки зрения архитектора ПП нужно тщательно обдумать модель угроз, модель нарушителя, границы доверия системы и др.;

4) создать правила, пособия, стандарты по обеспечению информационной безопасности;

5) реализовать эффективные механизмы протоколирования, аудита и мониторинга.

Рассмотрим сам процесс создания программного продукта (ПП). Его можно разделить на два этапа: 1) разработка – development (Dev); 2) поддержка, использование – operations (Ops). Внедрение процессов ИБ лучше начинать с самого начала создания программного продукта.

На этапе разработки (Dev) выделим следующие элементы, в которых возможно контролировать процесс с точки зрения ИБ:

1) персональный компьютер (ПК) разработчика;

2) репозиторий локальный на ПК разработчика;

3) репозиторий центральный на выделенном сервере, внешнем или внутреннем.

Параллельно с процессом Dev идет процесс поддержки и администрирования ПП (Ops), в котором выделим также элементы, в которых можно контролировать процесс с точки зрения ИБ: 1) CI/CD-сервер; 2) серверы управления инфраструктурой.

Авторами разработан перечень процессов ИБ, выполнение которых необходимо при разработке ПП, сущность этих процессов раскрывается структурой их подпроцессов [6].

1 – Управление исходными данными (Source control):

1.1. контроль кода приложения (требования и рекомендации);

1.2. контроль кода инфраструктуры (требования и рекомендации);

1.3. просмотр всех изменений (code review) другим разработчиком;

1.4. запрет команды репозиторию исходного кода для мониторинга изменений исходного кода (commit) из папки с разрабатываемым/новым кодом (feature branch) в главную папку с исходным кодом разработанного ПО (master branche).

2 – Разворачивание (установка) установочного пакета/ контейнера на существующую инфраструктуру-сервер (Build):

2.1 просмотр и тестирование задач, запланированных процессов (Jobs) на комплектацию в master branch;

2.2. регистрация всех изменений в коде (build jobs);

2.3. организация доступа сервера, который автоматизирует процесс установки установочного пакета/ контейнера (Build – сервера), только к разрешенным библиотекам.

3 – Работа с репозиторием и версиями приложений (Repository work):

3.1. отсутствие прямого доступа к бинарным файлам;

3.2. сканирование репозиториев.

4 – Проверка качества (Quality Assurance, QA, например, при помощи Sonar, Fortyfy, checkmark и т.д.):

4.1. разрешение разворачивания (установки) установочного пакета/ контейнера (build) на инфраструктуре только после успешного сканирования исходного кода – SAST (Static Application Security Testing – сканер исходного кода);

4.2. проверка конфигурации сканера исходного кода (SAST, Static Application Security Testing);

4.3. возможность прослеживания каждого сценария тестирования функциональности (Function-теста) и наличие описания сценария на человекоподобном языке (user story);

4.4. необходимость подтверждения сценариев тестирования владельцем продукта – лицом от заказчика (PO, Product owner);

4.5. обязательное сохранение всех результатов тестов и обязательный их просмотр PO;

4.6. возможность внесения изменений в задачи и сценарии тестирования (test case) только ключевой командой разработки (core (dev) team);

4.7. обязательное тестирование ключевых функций приложения;

4.8. обязательное утверждение тестов безопасности (Security test, Sec test) PO и Test team lead для инфраструктурного кода;

4.9. обязательное утверждение Sec test PO и руководителем группы тестирования (Test team lead) для кода приложения;

4.10. обязательное ознакомление с результатами тестов PO и руководителя проекта.

5 – Реализация на непродуктивный сегмент (синтетические данные (сегмента), которые нужны для проверки разрабатываемого продукта) (Unproductive segment deploy):

5.1 проверка скриптов/кодов (code review) деплоя (реализации) и конфигурации;

5.2 отсутствие связи с продуктивной средой;

5.3 использование непродуктивных данных.

6 – Реализация на продуктивный сегмент (реальные данные (сегмента), которые защищаются) (Productive segment deploy):

6.1 прохождение проверки кодов реализации (code review) и конфигурации (плюс ручной режим опционально);

6.2 обязательное подтверждение/ просмотр окончательной версии и результатов тестов PO;

6.3 каждая реализация должна иметь разрешение (ордер) на изменения;

6.4 автоматизированный откат;

6.5 отсутствие связи с непродуктивным окружением.

7 – Поддержка (Support):

7.1 доступность разработок только для чтения (read only) в среду разработки;

7.2 обязательное прохождение изменения кода через автоматический пайплайн (конвейер, подразумевающий непрерывный процесс CI/CD; pipeline);

7.3 обеспечение контроля доступа к любой из сред (например, Dev, test, prod).

На рисунке 1 представлена разработанная авторами реализация защиты информации на всех этапах и подэтапах процесса разработки ПП (DevSecOps).

Подэтапы разработки ПП выполняются последовательно, при этом процессы и подпроцессы ИБ могут выполняться как последовательно, так и параллельно в рамках каждого подэтапа.

Первый подэтап разработки ПП «Разработка» включает в себя следующие процессы и подпроцессы ИБ:

– Процесс № 1 – Управление исходными данными (Source control): подпроцессы 1.1-1.4.

– Процесс № 2 – Комплектация (Build): подпроцессы 2.1-2.3.

– Процесс № 3 – Работа с репозиторием и версиями приложений (Repository work), подпроцессы 3.1-3.2.

– Процесс № 4 – Проверка качества (QA, Quality Assurance): подпроцессы 4.1-4.2.

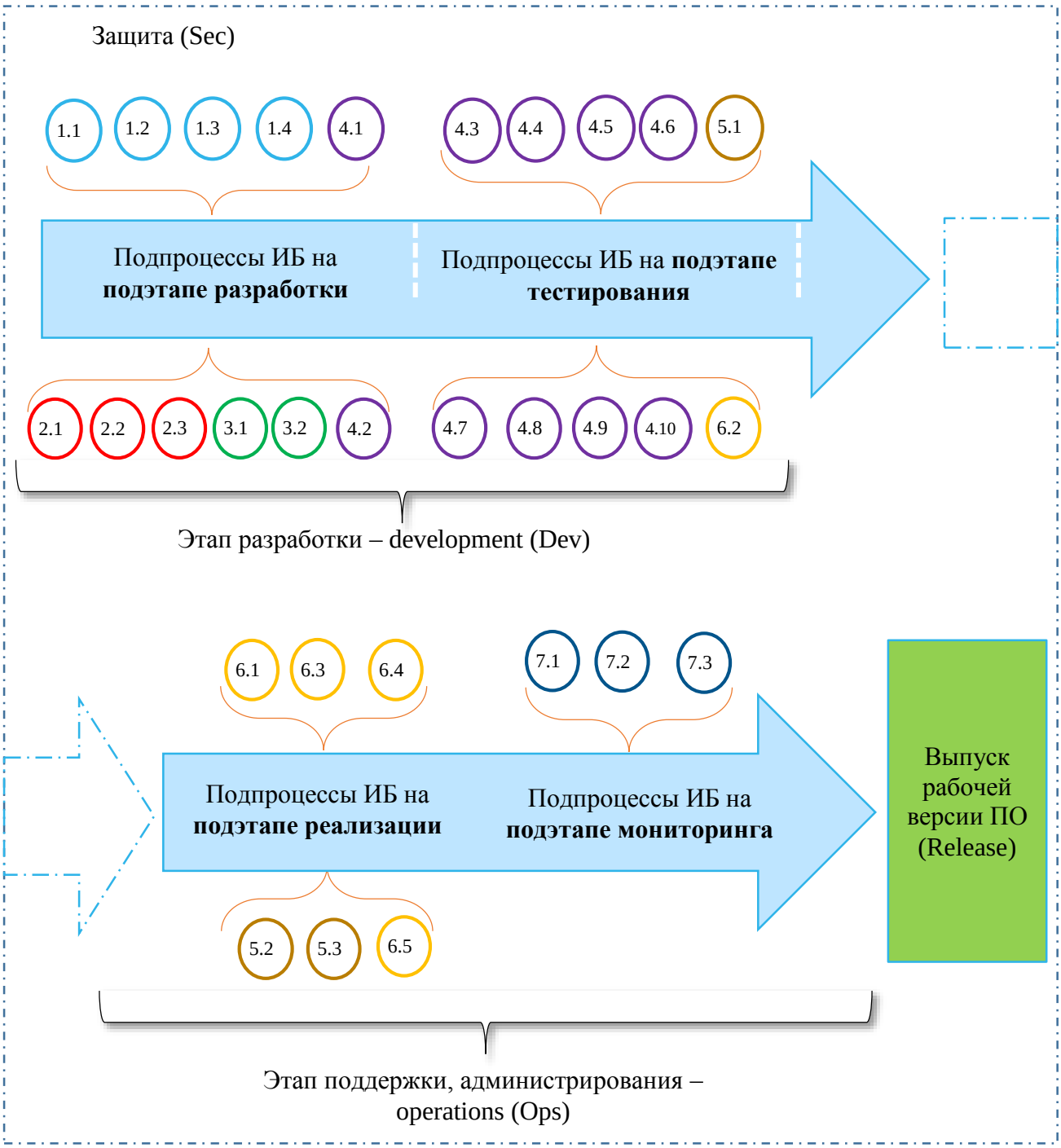

Рисунок 1 – Реализация ИБ на всех этапах процесса разработки ПП (DevSecOps)

Второй подэтап разработки ПП «Тестирование» включает в себя следующие процессы и подпроцессы ИБ:

– Процесс № 4 – Проверка качества (QA, Quality Assurance): подпроцессы 4.3-4.10.

– Процесс № 5 – Реализация на непродуктивный сегмент (Unproductive segment deploy): подпроцесс 5.1.

– Процесс № 6 – Реализация на продуктивный сегмент (Productive segment deploy): подпроцесс 6.2.

Третий подэтап разработки ПП «Реализация» включает в себя следующие процессы и подпроцессы ИБ:

– Процесс № 5 – Реализация на непродуктивный сегмент (Unproductive segment deploy): подпроцессы 5.2-5.3.

– Процесс № 6 – Реализация на продуктивный сегмент (Productive segment deploy): подпроцессы 6.1, 6.3-6.5.

Четвертый подэтап разработки ПП «Мониторинг» включает в себя следующие процесс и подпроцессы ИБ:

– Процесс № 7 – Поддержка (Support), подпроцессы 7.1-7.3.

Перечислим действия, которые команда-разработчик ПП в рамках подхода DevSecOps (гибкая команда) должна предпринять, чтобы доказать прослеживаемость и гарантии безопасности при разработке ПП.

1. Гибкая команда, чтобы соответствовать нормативным требованиям, хранит сведения о каждой функции и каждом изменении: кто запросил, кто утвердил и согласованные критерии приемки (т.е. условия, при которых заказчик будет удовлетворен). К услугам современных команд имеются инструменты управления проектом или трекеры историй, например, Rally Version One или Jira, которые ясно показывают, чем команда занимается сейчас и что она уже сделала с точки зрения аудитора.

2. Гибкая команда совместно с группой соответствия нормативным требованиям согласует определение готовности, включив в него факты, необходимые для доказательства соответствия историй, спринтов и релизов.

3. Все рабочие материалы: код приложения, конфигурационные рецепты и шаблоны, тесты, политики, документация (за исключением секретной и/или конфиденциальной), записываются в систему управления версиями с отсылкой к конкретному требованию, запросу изменения или извещению об ошибке (по идентификатору истории, номеру заявки или еще какому-то идентификатору, который можно указать в комментарии при записи в репозиторий). В результате формируется подробная история всего, связанного с каждым изменением.

4. Фильтры записи в репозиторий автоматически сканируют код на наличие секретов и небезопасных вызовов, перед тем как объединить его с главной ветвью.

5. Все изменения кода и конфигурации инспектируются (до записи в репозиторий), и результаты инспекции становятся видны команде. Для этой цели применяются запросы на включение Git или инструменты коллективной инспекции кода типа Gerrit или Review Board. Инспекторы сверяются с контрольными списками, проверяя, что код отвечает принятым в команде стандартам и наставлениям, и обращая внимание на небезопасное кодирование. Руководство периодически проводит аудит, чтобы подтвердить, что инспекции проводятся надлежащим образом и что программисты не просто проштамповывают работу коллег.

6. Каждое изменение (кода приложения и конфигурации) проходит стадию тестирования: разработка через тестирование, статический анализ кода и другие виды сканирования, а также автоматизированное приемочное тестирование. Автоматически измеряется тестовое покрытие. В случае серьезных проблем сборка прерывается. Поскольку тесты хранятся в репозитории исходного кода, их можно проинспектировать, сопоставить с критериями приемки каждой истории и убедиться, что требования были реализованы правильно.

7. Код (в т.ч. и код зависимостей) и инфраструктура регулярно сканируются на наличие уязвимостей, поскольку это часть автоматизированного конвейера. Сведения о найденных уязвимостях фиксируются и направляются в журнал пожеланий команды для исправления.

8. Изменения автоматически подвергаются приемочному тестированию, затем переносятся в промежуточную технологическую среду и, если все тесты и проверки прошли, поступают в производственную среду, так что можно увидеть, когда изменение попало в каждую среду и как это происходило.

9. Системы регулярно проверяются на наличие неавторизованных изменений с помощью программ обнаружения изменений (например, Tripwire или OSSEC).

Таким образом, выполняя выше перечисленные действия, в любой момент можно сказать, когда были внесены изменения и исправлены ли уязвимости. Если в процессе разработки ПП имел место нежелательный результат, то можно точно проследить, что именно было изменено, и быстро исправить ошибку. Это эффективно и с точки зрения контроля, потому что можно проследить каждое изменение и удостовериться в том, что все изменения вносятся единообразно и ответственно; и с точки зрения соответствия нормативным требованиям. Следовательно, все действия можно доказать аудиторам проекта.

Чтобы управлять изменениями, которые появляются каждые несколько секунд, нужно с самого начала устранить риск, прогоняя каждое

изменение через совокупность тестов и проверок; и оптимизировать, выполняя изменения небольшими порциями. В DevOps изменения в основном небольшие, с низким риском. Можно считать, что это стандартные или рутинные изменения, которые заранее одобрены руководством и не требуют созыва полномасштабного совещания команды разработчиков ПП.

В результате внедрения предлагаемого гибкого подхода к разработке ПП с обеспечением процессов ИБ была существенно увеличена скорость выпуска ПП за счет внедрения непрерывных автоматизированных процессов. При этом значительно сократилось время получения прибыли за счет экономии на простоях и перерасходе ресурсов на этапах ожидания, т.к. при возникновении инцидента ИБ показатель предотвращенных потерь был значительно уменьшен. При возникновении инцидента ИБ значение показателя предотвращенных потерь дает возможность оценить качество ПП.

Список литературы

1. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 года № Пр-646 [Электронный ресурс]. URL: http://www.consultant.ru/ document/cons_doc_LAW_208191/ (дата обращения: 10.09.2019).
2. Указ Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]. URL: http://www.consultant.ru/document/ cons_doc_LAW_216363/ (дата обращения: 10.05.2019).
3. Манифест гибкой методологии разработки программного обеспечения. [Электронный ресурс]. URL: https://agilemanifesto.org/iso/ru/ manifesto.html (дата обращения 01.08.2019).
4. Agile Alliance. What is Agile Software Development? [Электронный ресурс]. URL: https://www.agilealliance.org/agile101/ (дата обращения 02.08.2019).
5. Manifesto [Электронный ресурс]. URL: https://www.devsecops.org/ (дата обращения 10.10.2019).
6. Майорова Е.В., Соколовская С.А., Черток А.В. Преимущества гибкого подхода для сопровождения проектов разработки программного продукта // Петербургский экономический журнал: научно-практический рецензируемый журнал. – 2019. № 4. – С. 15-24.

УДК 004.056

Информационная безопасность систем управления современного автотранспорта с точки зрения потенциальной возможности реализации внешних угроз

С. К. Морозов, старший преподаватель,
Е. В. Красильникова, к.т.н., доцент,
Санкт-Петербургский государственный экономический университет

Внедрение автоматизированных систем управления автомобилем на основе микропроцессорных технологий, в том числе с использованием технического искусственного интеллекта, по нашему мнению, в целом является положительным явлением. Причины этого кроятся в особенностях процесса управления современным автотранспортом, где важным фактором для безаварийной эксплуатации является реализация функций курсовой устойчивости, динамической стабилизации автомобиля, в том числе в сложных дорожных условиях. Одновременно это позволяет уменьшать влияние человеческого фактора либо полностью устраняя его, либо частично компенсируя в ряде отдельных процессов, связанных с управлением автотранспортным средством, в том числе по безопасным маршрутам.

Но массовое внедрение данных технологий порождает определенный набор проблем, которые нельзя оставить без внимания. В современных автомобилях в угоду тенденциям интеграции и тотального снижения себестоимости отсутствует резервный контур управления. До определенного момента данная проблема решалась на уровне высоконадежных механических связей в контуре рулевого управления и элементах автоматики.

Известны отдельные случаи, когда неконтролируемый разрыв потока мощности, передаваемый от двигателя к ведущим колесам, в процессе выполнения такого опасного маневра, как обгон приводил к очень тяжелым дорожно-транспортным происшествиям. Причиной подобных явлений часто становилась не механическая неисправность узлов автомобиля, а нарушение логики работы системы управления «двигатель-коробка передач» при случайных сбоях микропроцессорных систем управления.

Современный дорогой автомобиль имеет до 90 электронных регулирующих блоков. Они придуманы для того, чтобы помогать водителю, или даже заменять его. Проблема в том, что они далеко не всегда работают так, как задумано, а, порой, становятся причиной аварии [2].

Не всегда электронные ассистенты, компьютеры, помогающие водителю и даже, заменяющие его работают так, как задумано. Порой, именно

электроника становится причиной аварии. Так, недавно в «Мерседесе» электроника отказалась работать и выключила мотор, когда машина была в узком тоннеле, имевшем лишь две полосы движения – одна туда, другая навстречу. Только чудом водителю удалось избежать аварии [2].

Или другая история, обошедшая все СМИ. Водитель автомобиля Renault Vel Satis, находясь за рулем, позвонил в полицию и сообщил, что у него не выключается темпомат (круиз-контроль) – компьютерное устройство, самостоятельно регулирующее подачу газа. Водитель, включив темпомат, должен только рулить – все остальное машина делает сама. Этот водитель задал темпомату скорость 130 км в час, но в одном месте, когда он пошел на обгон и развил скорость 190 км в час – устройство отказалось подчиняться – водитель не мог ни остановиться, ни медленнее ехать, хотя обычно темпомат должен отключаться, как только водитель начинает тормозить. Он попытался отключить это устройство – не тут-то было. В нормальной машине, в худшем случае, нужно повернуть ключ зажигания. В этой же машине ключа нет – там стоит некая карточка, которую, как сообщил водитель, заклинило и он не может ее вынуть. Француз сказал полицейским, что он давит ногой на тормоз, но все напрасно – машина несется, не сбавляя скорости. Эта гонка продолжалась около часа. Сообщалось, что кончилось все так же неожиданно, как и началось, водитель каким-то образом сумел вернуть себе контроль над разбушевавшейся машиной [2].

По статистике примерно треть отказов – это отказы электроники. Так, недавно DaimlerChrysler отозвал на проверку 680 тысяч мерседесов Е-класса из-за того, что у них возникли проблемы с электронной системой тормозов SBC [2]. Компания BMW в экстренном порядке предупредила, что выпущенные в определенный временной промежуток автомобили 5-й, 6-й, 7-й и x5 серий могут неожиданно отказать мотор, тормоза и усилитель руля [2].

По заявлению представителя автоконцерна Volkswagen вполне можно представить уже в обозримом будущем колонну беспилотных грузовиков, отправляющихся по автобану из одного логистического центра в другой [3].

Подобные проблемы могут проявляться в системах с электрическим и электрогидравлическими усилителями, где есть следящая микропроцессорная система. Также сбои возможны в контурах управления газом и рулевого управления.

Особую опасность для микропроцессорных систем управления может представлять реализация преднамеренных деструктивных электромагнитных воздействий, которой способствует бесконтрольное распространение некоторых устройств и их описаний в интернете.

Существует большая вероятность, что ГИБДД получит новый способ борьбы с угонщиками и нарушителям правил дорожного движения (ПДД). Полицейские смогут дистанционно отключать зажигание у преследуемого автомобиля, что может быть потенциально реализовано на основе системы «ЭРА-ГЛОНАСС». Речь идет не только об отключении двигателя у автонарушителя, но и об установлении тотального контроля за соблюдением ПДД: благодаря «ЭРА-ГЛОНАСС» траектория движения транспортного средства будет записываться с высокой точностью [4]. Разрабатываемые и реализуемые подходы дистанционной блокировки агрегатов двигателей могут позволить предотвращать серьезные последствия преступной деятельности.

Но реализация подобной технологии борьбы с противоправными действиями должна обеспечиваться защищенными каналами связи с использованием соответствующих протоколов обмена данными. Закрытие каналов должно производиться на техническом и/или криптографическом уровне для отсутствия возможности постороннего вмешательства в данный контур управления со стороны злоумышленников и предотвращения появления нового вида угроз. При этом должен быть установлен жесткий регламент на использование такого вида воздействий с учетом последствий для третьих лиц. А также должен быть определен круг имеющих право на осуществление такого вида воздействий, должно производиться детальное протоколирование их применения и определена ответственность в случае их несанкционированного применения.

Список литературы

1. Гуревич В.И. Уязвимости микропроцессорных реле защиты: проблемы и решения. – М.: Инфра-инженерия, 2016. – 256 с.
2. Электронные ассистенты решают проблемы и создают их / 2500 человек в год - жертвы диких животных, 19.11.2004 [Электронный ресурс]. URL: https://www.dw.com/ru/электронные-ассистенты-решают-проблемы-и-создают-их-2500-человек-в-год-жертвы-диких-животных/a-1404184 (дата обращения: 10.11.2019).
3. Автономное вождение для автопрома Германии не самоцель, а средство [Электронный ресурс]. URL: https://www.dw.com/ru/автономное-вождение-для-автопрома-германии-не-самоцель-а-средство/a-51070493 (дата обращения: 10.11.2019).
4. Полиция сможет отключать двигатель у преследуемого автомобиля [Электронный ресурс]. URL: https://newsland.com/community/5652/ content/politsiia-smozhet-otkliuchat-dvigatel-u-preslеduemogo-avtomobilia/5190567 (дата обращения: 10.11.2019).

УДК 004.056

Алгоритм (этапы) создания системы обработки и обеспечения безопасности персональных данных в организации

В. Г. Петров, к.т.н., доцент,
ведущий специалист отдела информационной безопасности АО «Научно-производственное предприятие «Радар ммс»

В связи с принятием Федерального закона от 27.07.2006 N 152-ФЗ (в редакции ФЗ от 25.07.2011 № 261) «О персональных данных» (далее 152 ФЗ) в подавляющем большинстве организаций возникают проблемы с созданием системы обработки и обеспечения безопасности персональных данных (далее ПДн). Это можно объяснить либо отсутствием в организации специалистов в области защиты информации, либо низким уровнем квалификации таких специалистов, либо просто нежеланием руководства решать эту проблему. Однако решать ее необходимо. В противном случае могут возникнуть проблемы уже другого рода, а именно при реализации своих полномочий Роскомнадзором в части применения статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

Как следует из указанного 152 ФЗ, с персональными данными осуществляются два действия, а именно: обработка персональных данных и обеспечение их безопасности.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [1].

Политика безопасности (информации в организации): совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [2].

Безопасность информации [данных]: состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность [2].

Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2].

Доступность информации [ресурсов информационной системы]: состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [2].

Целостность информации: состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. [2].

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными [1].

Не вдаваясь в подробности при описании требований 152 ФЗ, следует отметить, что главной задачей оператора является создание системы обработки и обеспечения безопасности персональных данных.

Указанным ФЗ определены обязанности и права оператора и субъекта ПДн. В частности, оператор обязан сформировать систему обработки и обеспечения безопасности персональных данных (далее - СООБ ПДн).

Как известно, любая система содержит три главные компоненты: люди, документы, техника. Люди – сотрудники (работники) организации, подготовленные в профессиональном отношении к выполнению возложенных на них задач. Документы – организационно-распорядительные документы (ОРД), разработанные на основе нормативных правовых актов РФ, нормативных правовых актов, руководящих и методических документов различного рода регуляторов, в том числе ГОСТы, и предназначенные для формирования и организации функционирования СООБПДн. Техника – средства вычислительной техники (СВТ) и технические средства защиты информации (СЗИ), которые составляют техническую основу информационных систем персональных данных (ИСПДн).

В результате анализа содержания нормативных правовых актов, нормативных и методических документов, действующих в области персональных данных и иной информации конфиденциального характера, а также учитывая опыт работы в сфере защиты информации, автором предлагается рассмотреть и, в случае необходимости, использовать в практической деятельности приведенный ниже алгоритм создания СООБПДн.

Алгоритм можно условно разбить на 3 этапа. Причем мероприятия различных этапов можно выполнять одновременно, а не обязательно последовательно, если это не вызывает каких-либо противоречий.

<u>На первом этапе</u> следует провести организационные мероприятия, а именно:

– Назначить сотрудника(ов) из состава руководителей, ответственного(ых) за организацию мероприятий по обработке и обеспечению безопасности ПДн [1,3].

– Назначить ответственных за выполнение мероприятий по обработке и обеспечению безопасности персональных данных (подразделения,

сотрудники – специалисты по защите информации, администратор безопасности информации и пр.), определив при этом их функции, обязанности, права и ответственность в положениях о подразделениях и в должностных инструкциях сотрудников.

– Назначить комиссию по оценке соответствия (аттестации) объектов информатизации требованиям безопасности информации, по классификации автоматизированных систем и установке уровней защищенности персональных данных [4,5].

– Разработать организационно-распорядительные документы, определяющие содержание и порядок (политику) обработки и обеспечения безопасности персональных данных в организации [1-5].

В частности: «Положение об обработке и обеспечении безопасности персональных данных в организации». Указанным документом определяются правила (политика) обработки ПДн, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере ПДн, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых ПДн, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований [1].

В указанном Положении кроме правил обработки персональных данных должны быть представлены:

– комплекс мероприятий по обеспечению безопасности ПДн;

– правила рассмотрения запросов субъектов ПДн или их представителей;

– правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите ПДн, установленным 152 ФЗ, принятыми в соответствии с ним нормативными правовыми актами и организационно-распорядительными документами;

– правила работы с обезличенными данными;

– перечень информационных систем персональных данных;

– перечень персональных данных, обрабатываемых в организации;

– перечень должностей работников организации, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

– перечень должностей работников организации, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ним.

К указанному Положению целесообразно в качестве приложений разработать ряд перечней, инструкций и типовые формы различных документов.

– Перечень (состав) персональных данных, обрабатываемых в организации.

– Список должностных лиц, ответственных за организацию и выполнение мероприятий по обработке и обеспечению безопасности ПДн.

– Список должностных лиц, допущенных к обработке ПДн.

– Список должностных лиц, обеспечивающих безопасность ПДн.

– Список должностных лиц, обслуживающих ИСПДн.

– Должностные инструкции сотрудников, ответственных за организацию обработки и обеспечение безопасности ПДн.

– Должностные инструкции сотрудников, ответственных за выполнение мероприятий по обработке и обеспечению безопасности ПДн, допущенных к их обработке.

– Должностные инструкции сотрудников, обслуживающих ИСПДн.

– Перечень технических средств, участвующих в обработке ПДн, помещений, в которых они установлены, либо хранятся материальные носители ПДн, и лиц, допущенных в эти помещения.

– Порядок доступа работников в помещения, в которых ведется обработка персональных данных.

В качестве типовых форм документов могут быть разработаны:

– Обязательство сотрудников, непосредственно осуществляющих обработку ПДн, в случае расторжения с ними контрактов прекратить обработку персональных данных, а также о неразглашении персональных данных ставших известными им в связи с исполнением должностных обязанностей;

– Форма согласия субъектов ПДн на обработку его персональных данных;

– Форма согласия субъекта на получение его ПДн у третьей стороны;

– Форма согласия субъекта на передачу его ПДн третьей стороне;

– Форма запроса о предоставлении ПДн работников Предприятия (личных дел) для ознакомления;

– Форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои персональные данные;

– Форма заявления об отзыве согласия на обработку ПДн.

<u>На втором этапе</u> необходимо приступить к созданию ИСПДн в защищенном исполнении. При этом следует выполнить ряд мероприятий.

– Разработать частную модель угроз безопасности ПДн.

– Разработать модель нарушителя.

– Определить (установить) границы контролируемой зоны

– Определить (установить) уровень защищенности персональных данных.

– Определить (установить) класс защищенности ИСПДн как АС.

– Разработать техническое задание на создание ИСПДн в соответствии с ГОСТ 34602.

– Разработать техническое задание на создание системы защиты информации в ИСПДн в соответствии с ГОСТ 51583.

– Разработать проект на создание ИСПДн в защищенном исполнении.

В состав проектной документации, как правило, входят:

– пояснительная записка;

– структурная схема в виде чертежей;

– эксплуатационно-техническая документация.

В пояснительной записке излагаются сведения о:

– конфигурации и топологии ИСПДн в целом и ее отдельных компонентов;

– технических средствах и системах, предполагаемых к использованию в составе ИСПДн, в том числе средствах защиты информации, условиях их расположения;

– общесистемных и прикладных средствах программного обеспечения, предполагаемых к использованию в ИСПДн;

– технологии (режимах) обработки персональных данных в ИСПДн в целом и в ее отдельных компонентах;

– условиях расположения ИСПДн относительно ограждающих конструкций и границ контролируемой зоны.

На структурной схеме изображаются места расположения элементов ИСПДн:

– автоматизированных рабочих мест;

– линий связи между ними с привязкой к границам ограждающих конструкций;

– помещений и границй контролируемой зоны.

В спецификации к структурной схеме могут указываться типы ОВТ, типы соединительных проводов, типы разъемов и т.д.

Кроме этого может быть разработана принципиальная схема электрическая ИСПДн.

В состав эксплуатационно-технической документации, как правило, входят:

– инструкции по эксплуатации ИСПДн и АРМов, входящих в ее состав;

– руководство пользователю;

– инструкция системному администратору;

– инструкция администратору безопасности информации;

– инструкция по соблюдению правил техники безопасности (электро-, пожарной и т.д.);

– инструкция пользователю по соблюдению режима защиты информации при работе на АРМ и в ЛВС;

– инструкция пользователю о порядке отнесения информационных ресурсов Предприятия к защищаемым и об организации доступа к ним;

– инструкция пользователю в случае возникновения нештатных ситуаций;

– инструкция пользователям АРМ по организации антивирусной защиты;

– инструкция пользователям АРМ по организации парольной защиты;

– инструкция пользователю АРМ услугами электронной почты и internet;

– инструкция пользователю АРМ по использованию и хранению электронных носителей с информацией ограниченного доступа в подразделениях;

– инструкция по внесению изменений в списки пользователей АРМ и наделению их полномочиями доступа к информационным ресурсам Предприятия,

а также ряд иных, в случае необходимости, инструкций.

Второй этап завершается реализацией проекта, в процессе которого производится:

– закупка оборудования (СВТ, лицензионных программных продуктов, сертифицированных средств защиты информации, соединительных проводов, комплектующих изделий и т.д.)

– установка оборудования, прокладка кабелей и соединение элементов ИСПДн между собой, установка программных продуктов;

– настройка и отладка работы элементов и ИСПДн в целом;

– испытания и прием ИСПДн в эксплуатацию.

На третьем – заключительном этапе необходимо провести оценку эффективности реализованных мер защиты информации в ИСПДн.

Финальным документом при этом является «Акт по результатам оценки эффективности реализованных мер защиты информации» (Аттестат соответствия) с приложениями. Ниже приведен примерный состав приложений.

Акт установки уровня защищенности персональных данных.

Акт классификации АС (АРМ) в составе ИСПДн.

Предписание на эксплуатацию объекта информатизации – ИСПДн.

Схема (карта с границами) контролируемой зоны.

Протокол измерения параметров заземления АРМ.

Описание технологического процесса обработки информации (каким образом обрабатывается, что и где хранится, куда выдается и т.д.).

Технический паспорт объекта информатизации - ИСПДн.

Акт установки и настройки средств и систем защиты информации.

Матрица разграничения доступа к информационным ресурсам ИСПДн.

Состав программного обеспечения, установленного в ИСПДн.

Программа и методики аттестационных испытаний (в случае оценки эффективности реализованных мер защиты информации в ИСПДн в виде аттестации).

Сертификаты (копии) на установленные средства защиты информации (программные и технические).

Список лиц, имеющих доступ в помещение ОИ.

Заключение по результатам оценки эффективности реализованных мер защиты информации (аттестационных испытаний) в ИСПДн.

Разработка организационно-распорядительных документов - процесс творческий, который требует знаний, инициативы, значительных временных затрат.

Таким образом, в результате практической реализации рассмотренных этапов в организации создается и функционирует система обработки и обеспечения безопасности персональных данных, которая отвечает требованиям нормативных правовых актов РФ, нормативных правовых актов, руководящих и методических документов основных регуляторов в области защиты информации.

Список литературы

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (В ред. Федерального закона Российской Федерации от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»).
2. ГОСТ Р 50922-96 Зашита информации. Основные термины и определения.
3. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных».
4. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

УДК 004.77, 004.056

О проблемах развития концепции Интернета вещей

А. М. Полегенько, ведущий специалист по защите информации,
ЗАО «ТЕЛРОС»,
аспирант, Университет ИТМО,
старший преподаватель, Санкт-Петербургский государственный
экономический университет

Несмотря на стремительное развитие концепции «Интернет вещей» данное понятие в нашей стране вызывает множество вопросов и непонимания, особенно среди обычных пользователей. Зачастую пользователи фитнес трекеров, навигаторов или счетчиков электрических приборов даже не знают, что их устройства входят в сеть Интернета вещей, а тем более не задумываются об обеспечении их безопасности.

Анализ рынка Интернета вещей в России показывает недостаточные темпы роста по сравнению с ожидаемыми. Это проявляется в количестве SIM-карт, используемых для Интернета вещей – ожидаемый показатель с 23,5 млн. шт. снизился до 19 млн. шт. к концу 2019 года [1]. В первую очередь, такие показатели объясняют недостаточным финансированием, а также нехваткой приложений и их несовершенством.

Медленные темпы развития так же обусловлены сложностью стандартизации в этом секторе. Применение существующих стандартов и проколов не всегда возможно для устройств Интернета вещей, обладающих такими ограничениями, как размеры, производительная и вычислительная мощности, ресурсы памяти и др.

По масштабу сетей Интернет вещей можно разделить на следующие уровни:

1) уровень отдельных «вещей» (например, датчики и сенсоры, устанавливаемые независимо друг от друга для сбора информации об окружающей среде и телеметрии);

2) уровень «вещей», объединенных между собой в рамках небольшой сети (например, «смарт-дом» с набором гаджетов, взаимодействующих друг с другом в рамках одной домашней сети);

3) уровень «вещей», объединенных в рамках крупной сети (например, концепция «умного города»);

4) уровень глобального Интернета вещей, целью которого является объединение стран.

От устройств первого уровня не требуется выполнение множества различных функций, связанных, например, с самостоятельным анализом

полученных данных, с координацией разных датчиков или коммутацией взаимодействия между ними. Отсюда можно сделать вывод о том, что такие устройства могут не обладать большим набором протоколов взаимодействия, как устройства на уровне «умного города».

Еще одним из факторов медленного развития Интернета вещей является отсутствие понимания принципов построения сетей и их взаимодействия. В открытых источниках информации очень часто по запросу используемых в Интернете вещей протоколах в одной статье может содержаться информация одновременно и об используемых протоколах, и стандартах, и технологиях. В связи с чем происходит полное непонимание реализации концепции Интернета вещей, особенно для тех, кто только начинает поиск и анализ информации.

Целью данной статьи не являлось изложение основ учебника по теории сетей, но проблематика такова, что поиск информации по данной теме затруднен, а это, в том числе, является фактором замедления развития Интернета вещей в нашей стране в целом.

В зависимости от уровня устройств Интернета вещей используются беспроводные сети разных уровней: персональные сети, локальные сети, беспроводные сети городского масштаба и глобальные. На каждом из этих уровней принято использование своих технологий, удовлетворяющих потребностям взаимодействия устройств на данном уровне без ущерба, например, их быстродействию, энергопотреблению и безопасности.

Исходя из масштаба существующих сетей, общую структуру применения беспроводных технологий можно представить следующим образом (рисунок 1).

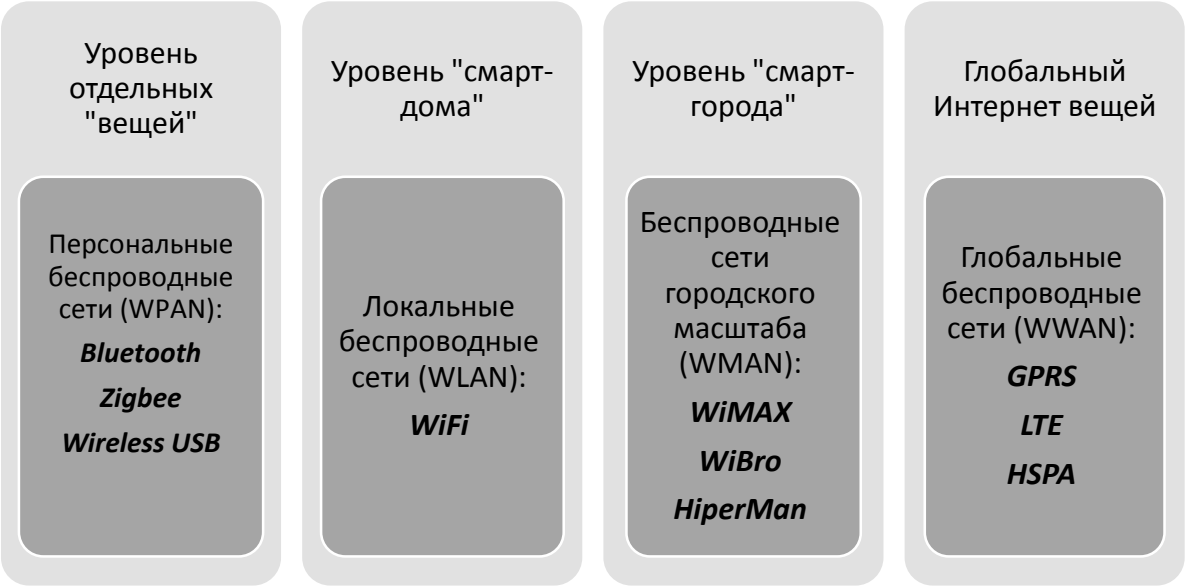

Рисунок 1 – Применение беспроводных технологий на разных уровнях Интернета вещей

Технологию Zigbee иногда так же рассматривают на уровне WLAN.

Персональные беспроводные сети характеризуются низким электропотреблением и малым радиусом действия, чем обусловлена их применимость в Интернете вещей. Многие из данных технологий не поддерживают межсетевые протоколы IP, и для взаимодействия с ними требуются либо специальные шлюзы, либо используются протоколы с надстройками, разработанные для обеспечения взаимодействия.

Таким образом, можно говорить о соответствии уровней устройств Интернета вещей стандартам беспроводных технологий в зависимости от масштабов и дальности работы устройств.

В зависимости от уровня сети архитектура Интернета вещей может включать в себя разные элементы, но классическое представление архитектуры включает в себя сами «вещи» (устройства), шлюзы, серверы и клиентскую часть – приложения (рисунок 2).

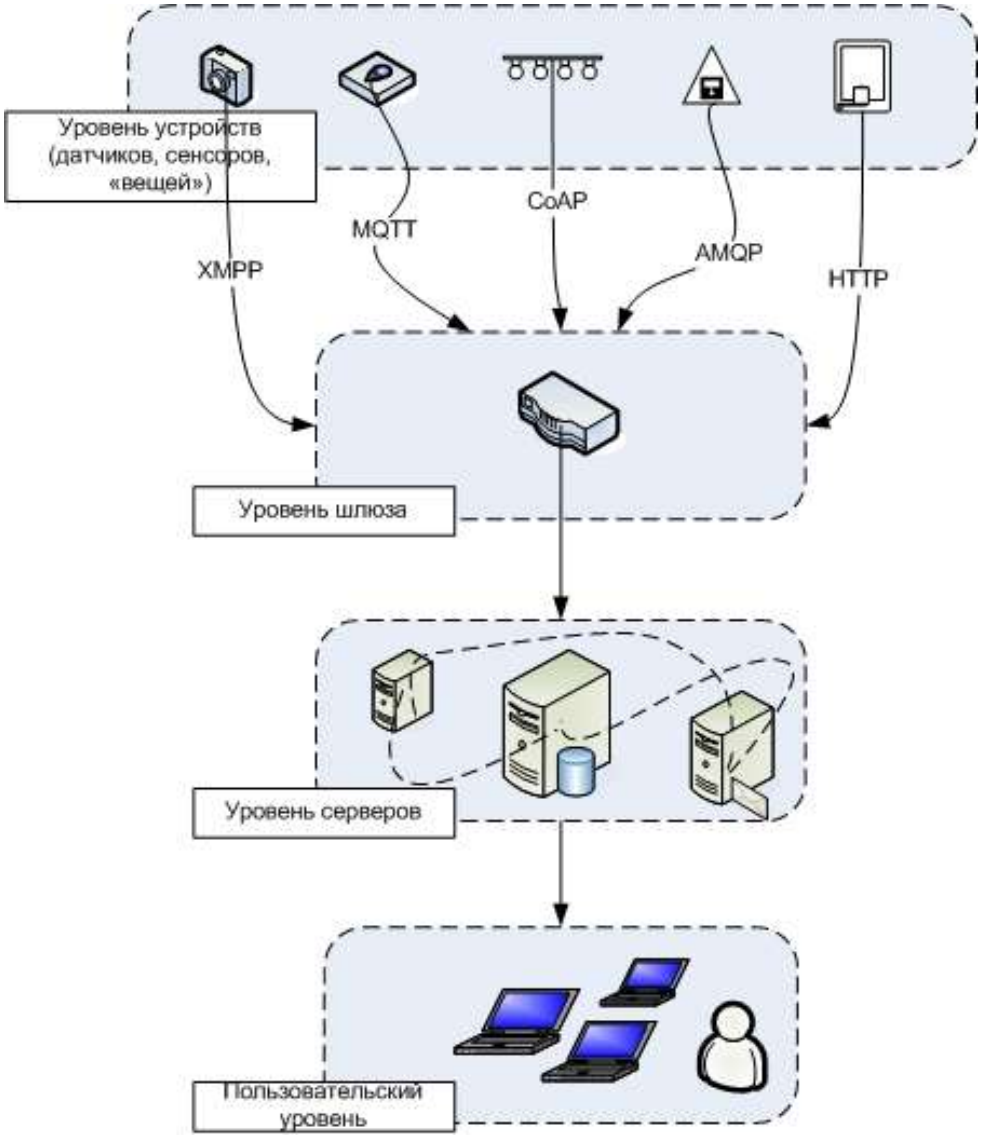

Рисунок 2 – Классическая архитектура Интернета вещей

Среди основных протоколов, применяемых в сети Интернета вещей, выделяют HTTP, MQTT, CoAP. В соответствии с исследованием IoT Developer Survey 2018, проведенным Eclipse IoT Working Group (подразделение Eclipse Foundation) совместно с AGILE IoT, IEEE и Open Mobile Alliance [2], протокол MQTT используется в 62,61% устройств, HTTP – в 54,1%, а CoAP – в 22,49%.

Протокол MQTT (англ. *Message queuing telemetry transport*) является оптимальным для использования в сети Интернета вещей. По сути, он и разрабатывался для таких сетей с целью сбора телеметрии от различных датчиков, характеризуется невысокой нагрузкой на сеть, простотой встраивания и использования.

Обмен по протоколу MQTT осуществляется по принципу «издатель-подписчик» (Publisher-Subscriber), при этом в отличие от клиент-серверной архитектуры издатель и подписчик, как правило, разделены, они не обязаны знать друг друга, не обязательно должны быть включены в одно время. Издатель и подписчик не передают друг другу сообщения напрямую, а управляет передачей стоящий между ними брокер. Например, издатель передает информацию о температуре окружающей среды, ставя при этом заголовок «Температура». Брокер, получая такие сообщения, анализирует, кто из подписчиков подписан на этот заголовок, и отсылает сообщение издателя – датчика температуры, только им.

CoAP (англ. *Constrained Application Protocol*) – бинарный протокол межмашинного взаимодействия, работающий поверх UDP, чем и отличается от HTTP, по образу которого разрабатывался.

Структура протокола CoAP основана на REST-архитектуре, т.е. позволяет строить приложения на основе группы методов – GET, PUT, POST, DELETE. CoAP легко интегрируется с HTTP для дальнейшего взаимодействия в сети с помощью CoAP-прокси. Например, датчики света, устанавливаемые в помещении, по запросу сообщением типа GET от HTTP-клиента через CoAP-прокси передают данные по протоколу CoAP о степени освещенности помещения.

Известнейший протокол HTTP так же является одним из лидеров по использованию устройствами Интернета вещей, как один из самых популярных протоколов сетевого взаимодействия, интеграция с которым не представляет собой сложностей.

Для обеспечения безопасности устройств сети Интернета вещей, в том числе, необходимо учитывать уязвимости используемых сетевых протоколов. Например, в устройстве Hickory Smart Ethernet Bridge производителя Belwith Products, LLC в июле 2019 года была обнаружена критическая уязвимость (CVE-2019-5635) [3], связанная с передачей данных в открытом виде по протоколу MQTT. Smart Ethernet Bridge является умным мостом между датчиками и клиентским приложением для мониторинга и управления. Данная уязвимость позволила получить логин и пароль пользователя MQTT-брокера.

Другая уязвимость была обнаружена в подсистеме MQTT в Gobot Hybrid Group до 1.13.0 версии (CVE-2019-12496) [3]. Gobot Hybrid Group – это фреймворк для робототехники и физических вычислений в Интернете вещей, предлагающий адаптеры и контроллеры для управления различными устройствами. Уязвимость связана с пропуском по умолчанию проверки корневых сертификатов CA.

Уязвимость CVE-2019-9750, обнаруженная в IoTivity – открытой платформе, обеспечивающей бесперебойную связь между устройствами Интернета вещей, заключается в подмене IP-адреса и реализации атак типа «отказ в обслуживании».

Это только единичные примеры уязвимостей протоколов, используемых в устройствах Интернета вещей.

На сегодняшний день развитие концепции Интернета вещей замедлено по ряду причин. В первую очередь, процедура стандартизации в области Интернета вещей в нашей стране проходит длительный путь с момента принятия стандартов до их применения в реальной жизни. Сравнительно недавно была принята «Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации» – в марте 2019 года, и только начинается процесс ее внедрения в разработку и эксплуатацию устройств Интернета вещей. С этой же проблемой тесно связана недостаточная информированность всех сторон-участников данного сегмента рынка. Многие потребители очень скептично относятся к таким новинкам, как умные лампочки, умные розетки и умные холодильники. Возможно, что для этого действительно есть основания – вопросы безопасности Интернета вещей пока остаются, в большинстве своем, открытыми. Обнаружение уязвимостей сетевых протоколов, связанных с работой умных устройств, происходит быстрее, чем принимаются стандарты и разрабатываются защищенные решения. Подход к обеспечению безопасности сетевого взаимодействия должен быть комплексным и системным и, в первую очередь, направлен на реализацию протоколов и использование сервисов, которые позволяют своевременно обновлять и поддерживать актуальные версии с возможными надстройками безопасности.

Список литературы

1. Интернет вещей, IoT, M2M мировой рынок, 21.08.2019 [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/ Статья:Интернет_вещей,_IoT,_M2M_(мировой_рынок) (дата обращения: 10.11.2019).
2. Щипко М., Костылев М. Как работает IoT: анализ технических решений. Часть 1, 21.02.2019 [Электронный ресурс]. URL: https://axmor.ru/blog/tehnologiya-iot-analiz-tehnicheskih-reshenij/ (дата обращения: 10.11.2019).
3. CVE. Common Vulnerabilities and Exposures [сайт]. URL: https://cve.mitre.org/ (дата обращения: 10.11.2019).

УДК 004.056

Метод оценки эффективности организации безопасного информационного взаимодействия элементов распределенной вычислительной сети

Ю. И. Синещук, д.т.н., профессор
Санкт-Петербургский университет МВД России

Современный этап развития человечества характеризуется формированием и развитием информационных систем и технологий, автоматизированных информационно-управляющих систем, трансграничных глобальных информационно-телекоммуникационных сетей. С технической точки зрения речь идет о формировании киберпространства (cyberspace), как некоторой виртуальной области, состоящей из взаимосвязанной сети инфраструктур, созданных на базе информационных технологий.

В последние годы для описания такого рода сложных, по сути, гибридных систем, включающих в себя, наряду с информационными, – физические объекты и процессы используется термин «киберфизические системы» (cyber-physical systems, CPS). CPS – это системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое. В CPS обеспечивается тесная связь и координация между вычислительными и физическими ресурсами. Компьютеры осуществляют мониторинг и управление физическими процессами с использованием такой петли обратной связи, где происходящее в физических системах оказывает влияние на вычисления и наоборот [1].

Предшественниками CPS можно считать встроенные системы реального времени, автоматизированные системы управления, отличительной особенностью которых является децентрализованная обработка информации, как наиболее эффективный способ повышения оперативности управления, реализуемый путем создания распределенных вычислительных систем (Distributed System, DS), в которых объединены между собой множество удаленных друг от друга ЭВМ или ВЦ.

DS представляет собою набор независимых компьютеров, который интерпретируется пользователями как единая объединенная сеть, ресурсы которой направленны на решение определенной общей задачи [2]. Особенностью DS является возможность разделения функций обработки и управления, а также обеспечение надежного и быстрого доступа пользователей к вычислительным и информационным ресурсам и организации коллективного использования этих ресурсов [2-5].

Динамика научно-технического прогресса требует постоянного развития DS при одновременном совершенствовании средств и систем обеспечения их безопасности. Необходимость обеспечения безопасности подразумевает выбор и реализацию рационального варианта безопасного информационного взаимодействия элементов DS.

Обоснование состава методов и средств защиты информации предполагает проведение предварительного анализа возможных угроз информационной безопасности. В общем случае, негативные воздействия на информационную систему, по своей природе, могут быть различными: внешние физические деструктивные факторы; внутренние деструктивные факторы, исследуемые в рамках анализа надежности; электромагнитные помехи; программно-информационные воздействия или кибератаки [6-8].

По сути речь идет об обеспечении кибербезопасности, подразумевающей, в числе прочих аспектов безопасности, организацию безопасного информационного взаимодействия в рамках киберпространства, формируемого элементами DS. Наличие разнообразных способов организации такого взаимодействия и средств обеспечения его безопасности, предполагает необходимость решения задачи оценки сравнительной эффективности. Характерные требования к оценке эффективности организацию безопасного информационного взаимодействия, как разновидности функционирования сложных систем, по целому ряду конфликтующих друг с другом показателей качества приводят к актуальной задаче многокритериальной оптимизации [9,10].

Задачи многокритериальной оптимизации в реальных условиях неполной определенности исходных данных могут быть решены различными методами [11].

Перспективным, в плане учета особенностей предметной области, является рассмотрение метода последовательных уступок (концессий, компромиссов) [12-14]. Метод предназначен для сравнительной оценки эффективности исследуемых систем по их показателям эффективности, заданных в количественной форме, а также в соответствии с расстановкой данных показателей по важности и их ограничениям (уступкам). Метод обеспечивает большую гибкость при сравнении систем, так как учитывает не только приоритет системы по тому или иному показателю эффективности, но и взаимосвязь показателей, и это является одним из главных преимуществ метода.

Практически все ведомства и организации стали проектировать свои автоматизированные информационно-управляющие системы(АИУС) на основе технических решений сетей Internet - Intranet. В организационно-техническом плане такие системы состоят из региональных и территориальных информационно-управляющих центров, оснащенных средствами автоматизации и передачи данных, и, по сути, являются разновидностью DS.

Взаимодействие различных подсистем ведомственных АИУС предполагает их подключение к ведомственной цифровой сети связи. Для обеспечения безопасного информационного взаимодействия возможны различные варианты такого подключения распределенных подсистем АИУС по выделенным каналам связи или через сеть Интернет с использованием средств защиты информации, например, ПАК ЗИ и ПК ЗИ семейства VipNet фирмы «ИнфоТекс»:

– вариант 1 (рисунок 1) – подключение через выделенный канал связи (возможно дополнительной использование ПАК ЗИ VipNet Coordinator HW 100).

– вариант 2 (рисунок 2) – подключение через Интернет с использованием ПАК ЗИ VipNet Coordinator HW 100.

– вариант 3 (рисунок 3) – подключение через Интернет с использованием клиентского ПК ЗИ VipNet Client.

При использовании первого варианта можно точно контролировать скорость передачи в канале, возможно подключение большого количества устройств, таких как компьютеры, устройства видеоконференцсвязи, IP-телефоны и т.д. Однако при этом необходимо учитывать расходы, связанные с абонентской платой за использование предоставляемого канала связи.

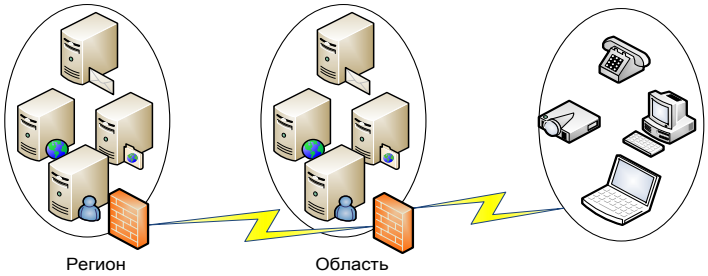

Рисунок 1 – Подключение через выделенный канал связи

Второй вариант также позволяет подключить большое количество различных устройств, создав подсеть за устройством ЗИ.

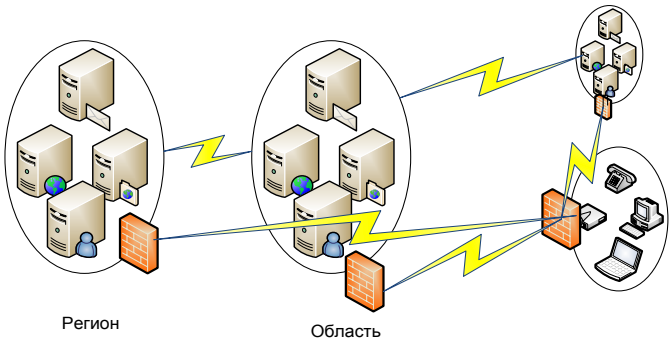

Рисунок 2 – Подключение через Интернет с использованием сетевых средств ПАК ЗИ (VipNet Coordinator HW 100)

Использование 3-го варианта, с применением клиентских средств ЗИ, существенно ограничивает варианты подключения, т.к. такие средства устанавливаются на персональный компьютер(ПК), и в этом случае на одном ПК придется совмещать все необходимые компоненты такие как IP-телефония, видеоконференцсвязь, доступ к FTP, электронная почта и т.д.

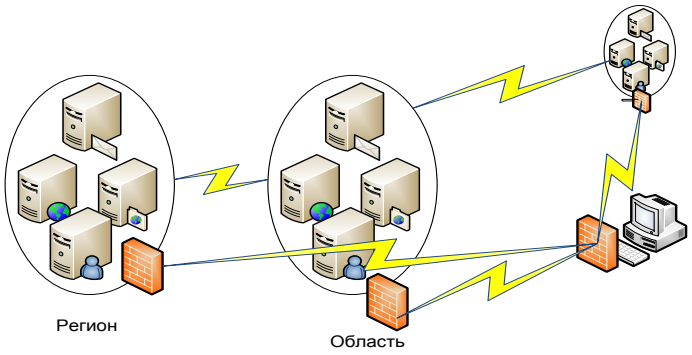

Рисунок 3 – Подключение через Интернет с использованием клиентских средств ПО ЗИ (VipNet Client)

Предъявление требований к организации взаимодействия на количественном уровне предусматривает определение показателей эффективности(ПЭ) и задание их предельных или интервальных значений. Учитывая информационный характер процессов в системе, в качестве базовых показателей могут быть предложены показатели производительности и безопасности. Кроме того, ориентируясь на требования функциональности использования ресурсов и сервисов DS предлагается, указанные базовые свойства добавить показателями, характеризующими количество предоставляемых сервисов, количество обслуживаемых рабочих мест, количество требуемого для эксплуатации персонала и стоимость эксплуатации.

Для полноты и объективности сравнительного анализа дополнительно анализировались варианты взаимодействия абонентов посредством телефонной сети и электронной почты. С высокой степенью уверенности можно предположить, что вышеперечисленные варианты могут являться базовыми при решении задач масштабирования DS АИУС.

В рассматриваемом примере многокритериальная задача выбора рационального варианта безопасного информационного взаимодействия формулируется в следующем виде. Дано множество допустимых альтернатив, каждая из которых оценивается множеством критериев. Требуется определить наилучшую альтернативу. При ее решении основная трудность состоит в неоднозначности выбора наилучшего решения. При этом отбор приемлемых вариантов производится на множестве решений, не улучшаемых ни по одному из критериев без ухудшения показателей по какому-либо из остальных.

Применение метода последовательных уступок предусматривает выполнение ряда процедур. Прежде всего, с помощью моделирования или методов экспертных оценок производится качественный анализ относительной важности показателей эффективности. Показатели располагаются и нумеруются в порядке убывания важности так, что главным является показатель ω_1, менее важным ω_2, затем остальные показатели: ω_3, ω_4, …, ω_n.

Далее максимизируется первый по важности показатель ω_1 – определяется его наибольшее значение W_1. Затем определяется (назначается) величина допустимого снижения (уступки) показателя ω_1 ($\Delta\omega_1 \geq 0$) и наибольшее значение второго показателя $\omega_2 \rightarrow W_2$ при условии, что значение первого показателя должно быть не меньше, чем W_1-$\Delta\omega_1$. Снова определяется (назначается) величина уступки, но уже по второму показателю – $\Delta\omega_2 \geq 0$, которая используется при нахождении условного максимума W_3 третьего показателя ω_3 и т. д. Наконец, максимизируется последний по важности показатель ω_n при условии, что (n-1) предыдущих должны быть не менее соответствующих величин W_i-$\Delta\omega_i$.

Полученная в результате совокупность показателей эффективности соответствует оптимальной системе или варианту ее построения.

Математическое решение задачи определяется следующей совокупностью последовательных действий:

$$\left.\begin{array}{l} 1)\ \mathrm{W}_1 = \sup \omega_1(x); \\ 2)\ \mathrm{W}_2 = \sup \omega_2(\mathrm{x}), \text{при } \omega_1(x) \geq W_1 - \Delta\omega_1; \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathrm{n})\ \mathrm{W}_n = \sup \omega_n(\mathrm{x}), \text{при } \omega_{n-1}(x) \geq W_{n-1} - \Delta\omega_{n-1} \end{array}\right\},$$

где sup – верхняя граница; $x \in X$ – множество значений технических характеристик.

В соответствии с математическим описанием метода последовательных уступок алгоритм его применения включает в себя следующие шаги (рисунок 4).

После выявления эффективной системы метод может применяться к оставшимся системам до полного выявления сравнительной эффективности всех рассматриваемых систем.

Содержательные этапы применения метода последовательных уступок к исследуемым вариантам представлены на рисунке 5.

Полученные результаты позволяют сделать вывод о целесообразности выбора варианта подключения взаимодействующих объектов через Интернет с использованием ПАК ЗИ VipNet Coordinator HW 100.

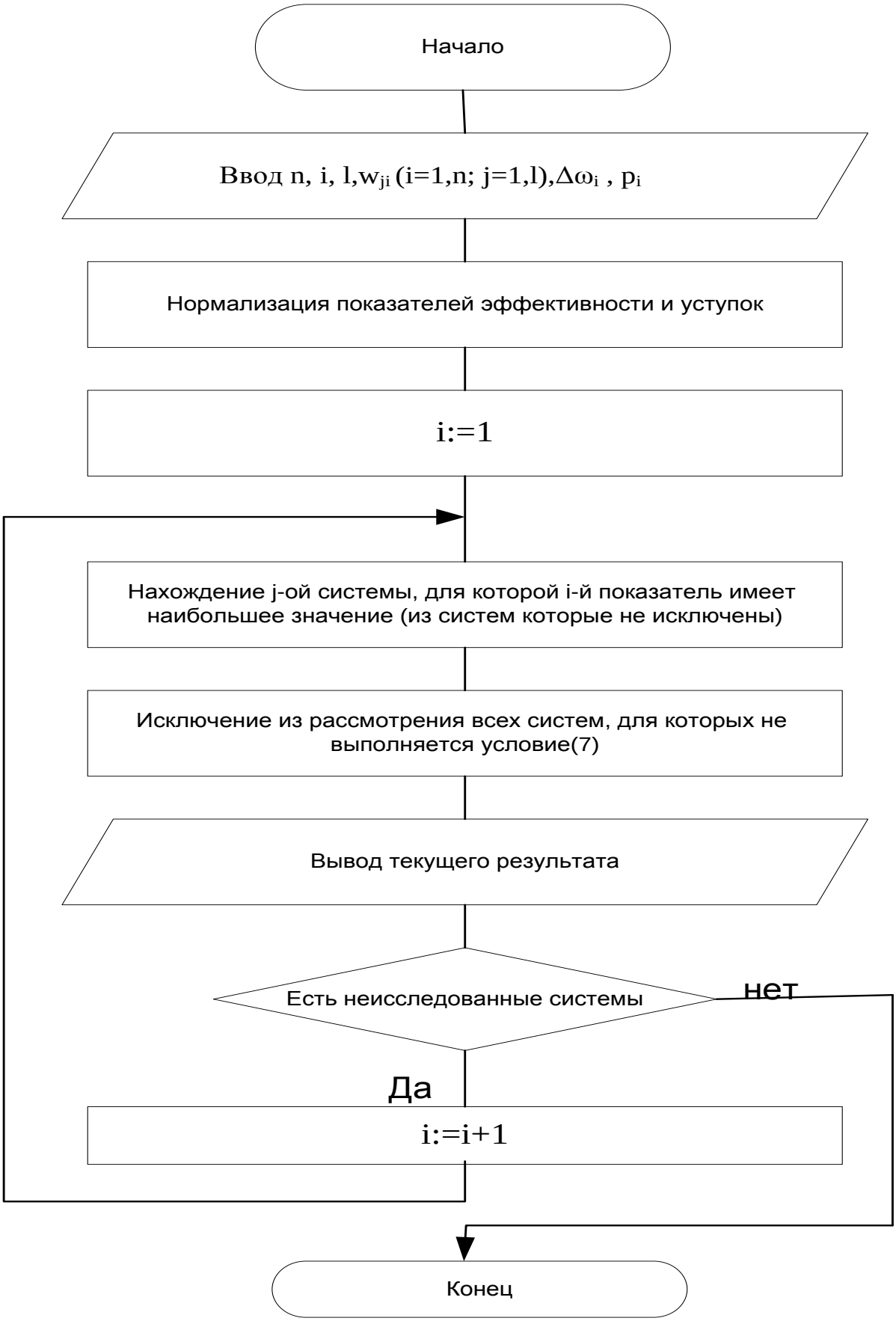

Рисунок 4 – Алгоритм метода последовательных уступок

вариант\показатель	Количество предоставляемых сервисов	Безопасность	Производительность (Мбит/сек)	Число рабочих мест	Стоимость содержания (т.руб.в год)	Количество специалистов
VipNet 100 (k)	4	0,9	20	10	170	3
VipNet 100 (i)	4	0,8	20	10	110	3
VipNet Cl	3	0,8	20	1	77	3
Email	2	0,4	10	1	60	2
Phone	1	0,2	0,5	1	24	1
индекс	0	0	0	0	1	1
уступка	2	0,1	10	2	120	2
Нормализация						
VipNet 100 (к)	1	1	1	1	0	0
VipNet 100 (i)	1	0,857142857	1	1	0,4109589	0
VipNet Client	0,666666667	0,857142857	1	0	0,6369863	0
Email	0,333333333	0,285714286	0,487179487	0	0,75342466	0,5
Phone	0	0	0	0	1	1
нормир. уступки	0,666666667	0,142857143	0,512820513	0,22222222	0,82191781	1
результаты шага №1						
VipNet 100 (k)	1	1	1	1	0	0
VipNet 100 (i)	1	0,857142857142	1	1	0,410958904	0
VipNet Cl	0,6666666666666	0,857142857142	1	0	0,636986301	0
результаты шага №2						
VipNet 100 (k)	1	1	1	1	0	0
VipNet 100 (i)	1	0,857142857142	1	1	0,410958904	0
VipNet Cl	0,6666666666666	0,857142857142	1	0	0,636986301	0
результаты шага №3						
VipNet 100 (k)	1	1	1	1	0	0
VipNet 100 (i)	1	0,857142857142	1	1	0,410958904	0
VipNet Cl	0,6666666666666	0,857142857142	1	0	0,636986301	0
результаты шага №4						
VipNet 100 (k)	1	1	1	1	0	0
VipNet 100 (i)	1	0,857142857142	1	1	0,410958904	0
результаты шага №5						
VipNet 100 (i)	1	0,857142857142	1	1	0,410958904	0

Рисунок 5 – Результаты применения метода последовательных уступок

Наилучшее условие для применения метода последовательных уступок складываются, когда количество сравниваемых систем приблизительно равно числу описывающих их показателей эффективности. Если число показателей больше количества систем, то возможны случаи, когда ряд показателей в процессе оценки использован не будет. Но так как, с одной стороны, это наименее важные показатели, а с другой – сравнение всех заданных систем оказывается выполненным, – считать это серьезным недостатком нельзя. Если количество систем больше числа показателей, то процесс содержит число шагов, равных числу показателей. И в этом случае задачу можно считать выполненной: отобраны лучшие системы по заданной совокупности показателей.

Список литературы

1. Edward A. Lee The Past, Present and Future of Cyber-Physical Systems: A Focus on Models, Sensors (Basel). 2015 Mar; 15(3) – P. 4837-4869.

2. Coulouris, George, Jean Dollimore, Tim Kindberg, Gordon Blair. Distributed Systems: Concepts and Design (5th Edition). Boston, 2011: Addison-Wesley, 1080 p.
3. Tanenbaum, E., Van Sten, M.: Distributed Systems: Principles and Paradigms, 2d edn., 2007, Prentice-Hall. – 686 p.
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.
5. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации: Учебник. 5-е изд. – М.: Финансы и статистика, 2014.
6. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) // Труды СПИИРАН, Выпуск 13. СПб.: Наука, 2010. ISBN 978-5-02-025507-4.
7. Синещук Ю.И. Примакин А.И., Яковлева Н.А. Основные угрозы и направления обеспечения безопасности единого информационного пространства. «Вестник Санкт-Петербургского университета МВД». – № 2. – 2013. – С. 150-154.
8. Синещук Ю.И., Яковлев О.В., Терехин С.Н. Информационный риск в условиях электромагнитного терроризма. Электронный научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». – № 3. – 2012. – с.15-18.
9. Интрилигатор М. Математические методы оптимизации и экономическая теория. М.: Прогресс, 1975. – 606 с.
10. Волкова, В.Н. Основы теории систем и системного анализа: учебник для вузов / В.Н. Волкова, А.А. Денисов. – 3-е изд. – СПб.: Изд-во СПбГТУ, 2003.
11. I. Kotenko, I. Saenko, Yu. Sineshchuk, V. Kuvatov, and O. Chudakov An Approach to Optimization of Information Security System Based on Accounting of the Prevented Damage Cost. Proceedings of ACM 12th International Conference on Security of Information and Networks, Sochi, Russia, September 2019 (SIN 2019), 8 pages.
12. Diallo A.B., Dim D.T., Bakasov S.R., Bogatikov V.N. Implementing «method of successive concessions» in selecting the optimal variant to protect a corporate network. The Eurasian Scientific Journal, [online] 1(10). (2018). URL: https://esj.today/PDF/25ECAVN118.pdf (дата обращения: 10.11.2019).
13. Mihail N. Yokhin, Maxim M. Stepanov. Application of the successive concessions method for optimizing the topology of information control systems with multiple-bus architecture. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 29 Jan.-1 Feb. 2018. – P.147-152.
14. Синещук Ю.И., Синещук М.Ю., Сысоев В.А. Метод последовательных уступок. Свидетельство о государственной регистрации программ для ЭВМ №2016612102, 18.02.16.

УДК 004.056

Особенности сбора информации о кандидате на должность сотрудника подразделения защиты информации на предприятии

А. В. Солодянников, к.т.н., доцент,
Санкт-Петербургский государственный экономический университет,
генеральный директор ООО «Ассоциация специалистов
по безопасности»

Самое сложное, что приходится делать руководителю любой организации, подбирать персонал. Подбор грамотных и квалифицированных работников является необходимым условием для нормального функционирования организации.

В производственном процессе нет мелочей, если работник обслуживающего персонала не справляется со своими обязанностями, то эффективность работы снижается, а что говорить о специалистах и руководителях.

Отбор персонала – основной этап в процессе формирования организации персоналом. На этом этапе формирования персонала руководство отбирает наиболее подходящих кандидатов из резерва, созданного в ходе набора. Естественно, выбирать следует человека, имеющего наилучшую квалификацию для выполнения данной работы на занимаемой должности, а не кандидата, который представляет наиболее подходящим для продвижения по службе. Объективное решение о выборе, в зависимости от обстоятельств, может основываться на образовании кандидата, уровне его профессиональных навыков, опыте предшествующей работы, личных качествах. Для руководящих должностей, особенно более высокого уровня, главное значение имеют навыки налаживания человеческих отношений, опыт руководящей работы. Эффективный отбор кандидатов представляет собой одну из форм предварительного контроля качества человеческих ресурсов.

Информация о кандидате на вакантную должность

Сбор информации о кандидате

В настоящее время отбор кандидатов на должности занимает в механизме управления персоналом особое место, поскольку весь коллектив предприятия является результатом отбора, ошибки, допущенные при отборе сложно исправлять, малорезультативный работник может дальше работать в организации и его будет сложно уволить.

Именно поэтому многие организации в работе с персоналом предпочитают сосредоточивать средства и усилия на отборе. Отбор среди кандидатов в таких организациях базируется на принципе: лучше не взять на работу нескольких подходящих кандидатов, чем принять одного неподходящего работника.

Часто, работая с кандидатом, специалист по персоналу сталкивается с такой ситуацией: по формальным признакам все подходит, интервью, тестирование, профессиональные испытания – все дает положительный результат. Но все же ясно, что это не «тот» кандидат. Профессионал умеет увидеть это и понять: все дело здесь именно в том, что организационная культура, в которой работал человек до этого, совсем иная, и он не сможет вписаться в данный коллектив.

Большинство нанимателей пытаются отбирать работников, во многом, судя о них по полученному ими образованию. Однако критерий образованности должен непременно сравниваться с требованиями работы.

Одной из важнейших персональных характеристик работника является его социальный статус. Некоторые работодатели предпочитают работников с высоким положением, другие – тех, кого интересует суть работы, а название должности для них не имеет значения.

Важной характеристикой также является возраст кандидата и его личностные особенности. Работодатели могут предпочитать общительных кандидатов замкнутым, и наоборот. Для решения определенных задач требуются те или иные личностные особенности.

Часто руководители затрудняются с формулировкой критериев. Специалисты по персоналу уточняют их, проговаривая особенности, элементы, ключевые моменты деятельности с руководителями. Бывает, что критерии не соответствуют друг другу или даже взаимно исключаемы. Это может осложнить отбор и даже сделать его невозможным.

Составление резюме и анкеты. В процессе набора кандидатов первым делом организации предлагают кандидатам на занятие вакантных мест представить свое резюме, в котором указываются личные сведения и основная информация об образовании, профессиональном опыте, имеющихся навыках и достижениях.

Кандидаты на какую-либо должность заполняют анкеты, специально разработанные отделом кадров или рекрутинговым агентством. Хотя они и не относятся к истинным средствам определения способностей, однако они тоже успешно применяются организациями для сравнительной оценки уровня квалификации. Пример заполнения такой анкеты приведен в следующей главе.

Собеседование. Другой вид сбора информации о кандидате - собеседование. Оно до сих пор является наиболее широко применяемым методом отбора персонала. Даже работников неуправленческого состава никогда не принимают на предприятие без хотя бы одного собеседования.

Важно помнить, что собеседование является двухсторонним процессом – не только организация оценивает кандидата, но и кандидат оценивает организацию с точки зрения ее соответствия его собственным интересам и запросам. Сотрудник отдела кадров или агентства должен предоставить

максимально объективную и полную информацию о предприятии, чтобы заинтересовать кандидата и, в тоже время, избежать приема нежелательных работников. Также многое о человеке может сказать и опоздание: насколько он опаздывает, предупреждает ли об опоздании и как объясняет его. Само по себе опоздание не считается преступлением и признаком того, что кандидат не годится. Его могут задержать объективные причины. Другое дело, как он говорит о них – как об обычной текучке, или жалуется, что мир вокруг него не организован.

Классификации собеседований.

– Биографические собеседования строятся вокруг фактов из жизни кандидата, его прошлого опыта. В ходе такого собеседования задаются такие вопросы:

– расскажите о своей прежней работе;

– почему Вы выбрали тот институт, в который поступили?

– Биографическое собеседование дает возможность оценить то, что кандидат уже сделал в своей жизни и на основании этого предположить, насколько успешно он сможет работать в должности.

– В ходе ситуационного собеседования кандидату предлагается решить практическую ситуацию. В качестве таковых часто ситуации, связанные с будущей профессиональной деятельностью кандидата. Проводящий собеседование сотрудник оценивает сам результат.

Критериальное собеседования представляет собой интервью, во время которого кандидату задаются вопросы о том, что бы он сделал в определенной ситуации (связанной с будущей профессиональной деятельностью), а его ответы оцениваются с заранее выработанных критериев.

Тестирование. Одним из способов уяснить, окажется ли кандидат соответствующим всем требованиям, и выбрать наиболее подходящего из группы кандидатов является тестирование претендентов в условиях, максимально приближенных к рабочим. Тестирование предназначено для оценки профессиональных, деловых и личностных качеств кандидата по результатам решения заранее подготовленных задач - тестов. Чтобы правильно составить и использовать тот или иной тест, необходимо, прежде всего, провести анализ рабочего процесса и выявить наиболее характерные черты, качества и стиль работы, которые позволяют быстро и эффективно выполнять именно эту работу. Тест должен быть составлен так, чтобы он позволял измерять или оценивать именно данные параметры, которые признаны важными или обязательными для занятия того или иного рабочего места или должности.

Интеллектуальные тесты. Интеллектуальные тесты предназначены для выяснения уровня интеллекта и образования кандидата. Могут использоваться как тесты общего интеллекта, так и специальные, направленные

на различные разновидности интеллекта. Например, для специалиста по рекламе и по связям с общественностью, важно обладать развитым вербальным интеллектом, уметь логично и грамотно изъясняться, обладать большим словарным запасом, точно понимать высказывания партнера. Для директора необходим высокий уровень аналитического мышления (умение анализировать и систематизировать большие объемы информации).

Тесты на внимание и память. Такие тесты могут быть включены в тест интеллекта, либо даваться отдельно, если эти навыки профессионально важны. Можно тестировать различные виды памяти, измерять ее объем и продуктивность запоминания.

Личностные тесты. Они предназначены для выявления личностных особенностей, черт характера, они описывают поведенческие особенности человека, его социальные навыки, способность к адаптации. Эти тесты могут выявлять уровень выраженности каждой характеристики или по совокупности данных относить человека к тому или иному типу. Существуют как комплексные тесты, описывающие личность в целом, так и тесты на какое-либо определенное качество (например, тесты на способность к самоконтролю, способ принятия решений, агрессию). Особо можно выделить тесты на выявления уровня мотивации (хочет ли человек реально работать или учиться, что может усилить его желание и подтолкнет на реальные действия и ценностные ориентации).

Тесты межличностных отношений. Эти тесты выявляют стиль общения с людьми, конфликтность, способность идти на компромиссы, приходить на помощь другим, навыки общения в различных ситуациях. Тестам на конфликтность уделяется особое внимание, поскольку сложные отношения в коллективе могут отнимать все рабочее время.

Источники информации о кандидате

Определенную помощь в том, чтобы избежать ошибок при отборе кадров, оказывают различные источники информации (таблица 1).

Резюме – это документально описанные основные данные биографии, профессионально-квалификационные характеристики, опыт работ, личностные качества.

Обычно резюме кандидатов содержит пробелы, касающиеся некоторых вопросов, связанных с биографией, личностными качествами специалиста. В подобных случаях используют важное дополнение -- специально составленную анкету, помогающую раскрыть ранее неизвестные сведения о кандидате.

Требования, предъявляемые к кандидатам

При приеме на работу выделяют следующие качества, присущие большинству хороших работников: развитое чувство ответственности, профессионализм, аккуратность.

Таблица 1 – Источники информации о кандидате на должность

№ п/п	Источники информации о кандидате	Содержание информации и значение
1	Заявление о приеме	Создает первое общее впечатление о кандидате
2	Фотография	Дает представление о внешности кандидата
3	Биография	Показывает процесс становления и развития личности, позволяет в некоторой степени узнать ее направленность
4	Личная анкета	Содержит важную систематизированную информацию о кандидате
5	Документы об образовании	Дают сведения об успехах в школе (вузе), но не позволяют судить о профессиональной квалификации
6	Трудовая книжка	Подтверждает места работы, указанные в биографии, освещает прежние сферы деятельности, описание квалификационной характеристики
7	Рекомендации	Освещают большинство аспектов профпригодности и личностных качеств
8	Интервью с кандидатом	Дает возможность заполнить существующие пробелы в информации, формирует личное представление о кандидате
9	Пробная работа	Определяет способность выполнять определенную работу и обладание определенными навыками
10	Медицинский осмотр на профпригодность	Позволяет определить физиологическую профпригодность к данному виду деятельности
11	Тесты	Позволяют получить характеристику некоторых личностных (интеллект, черты характера) профессиональных качеств

При определении конкретного профиля работы рабочего персонала необходимо учитывать характер возлагаемых на него обязанностей: объем работы, возможность нервной работы, возможность физической работы.

В принципе, на сегодняшний день при устройстве человека на работу его физические данные (сила, выносливость) не имеют решающего значения. Развитие технологии позволило значительно сократить ряд работ, для которых были необходимы физическая выносливость и сила. Приоритетное значение отдается умственным способностям личности, которые могут быть определены как способность эффективно использовать свой интеллект – сумму общих умственных функций понимания, мышления, обучения, наблюдения, решения проблем, способность вступать во взаимные отношения. Успешное обучение и сдача экзаменов обеспечивают определенный уровень умственных способностей, хотя некоторые работодатели могут дополнительно потребовать от предпо-

лагаемых кандидатов решить тесты на проверку уровня интеллекта, а также склонностей характера.

В контексте подбора на работу важны личностные качества работника, которые обычно означают комбинацию эмоций, мотивации, интересов; определенное их соотношение позволяет создать благоприятный микроклимат в коллективе, что будет способствовать, например, повышению производительности труда.

Требования, предъявляемые характером работы, особенностями профессии отражаются в профессиограммах, разрабатываемых специалистами на основе наблюдения за работником в процессе труда, включая проведение психофизиологических измерений, хронометража, фотографии рабочего времени. Профессиограмма – это описание особенностей определенной профессии, раскрывающее содержание профессионального труда, а также требования, которые она предъявляет к человеку (таблица 2).

Таблица 2 – Структура профессиограммы

№ п/п	Раздел	Содержание раздела
1	Профессия	Общие сведения о профессии, изменения, которые произошли с развитием производства, перспективы развития профессии
2	Процесс труда	Характеристика процесса труда, сфера деятельности и вид труда, продукция, орудия труда, основные производственные операции и профессиональные обязанности, рабочее место, рабочая поза
3	Санитарно-гигиенические условия труда	Работа в помещении или на воздухе, шум, освещение, режим труда и отдыха, льготы и компенсации, возможность производственным травм
4	Психофизиологические требования профессии к работнику	Требования к особенностям восприятия, мышления, внимания, памяти
5	Профессиональные знания и навыки	Перечень необходимых знаний, умений и навыков
6	Требования к повышению квалификации кадров	Формы, методы и сроки профессионального обучения, перспектива профессионального роста

На основании сравнения индивидуальных особенностей работника с нормативами профессиограммы можно сделать вывод о его соответствии и профессиональной пригодности к данному виду труда.

Нет такой организации, которая могла бы сказать, что ей не нужны профессиональные рабочие. Чтобы быть успешным работником, он должен обладать следующими данными.

– Возраст (предпочтение отдают молодым людям – они более активны).

– Образование (хотя главное в работе рабочего – хорошо разбираться в технологии, устройстве и материалах).

– Опыт работы (наличие опыта работы, особенно если человек работал на аналогичном производстве, знает его и представляет возможности работы).

– Личные качества. В каждой профессии, чтобы добиться успеха, надо обладать набором качеств. Для каждой профессии и должности существует баланс между опытом работы, образованием и личностными качествами. Обязательными являются: умение быстро устанавливать контакт с людьми, добросовестность, ответственность и порядочность.

Экспертная оценка документов

Оценка достоверности информации в документах, полученных от кандидата на должность

При получении документов о кандидатах кадровым специалистам важно не только получить какую-нибудь информацию о кандидате, но и оценить, насколько она соответствует действительности. Проверка достоверности сведений, предоставляемых кандидатами на вакантные должности, состоит в проверке рекомендаций и информации, указанной кандидатом в анкете или резюме, а также в предоставлении кандидатом справки о состоянии здоровья.

Проверка представленных документов, отзывов и рекомендаций является обязательной. Это поможет получить вполне объективную информацию для предсказания будущего поведения кандидата на рабочем месте.

Медицинский осмотр обычно проводится для определения возможностей кандидата физически выполнять предлагаемую работу, а также для предотвращения найма людей с инфекционными заболеваниями.

Рекрутинговое агентство или отдел кадров должны запрашивать у кандидата рекомендации в письменном виде от предыдущего работодателя с целью проверки его опыта работы. Эти рекомендации должны быть конфиденциальными. Также они наводят справки о предыдущих местах работы нового сотрудника.

За последнее время перед отделами персонала чаще стоит вопрос подбора не готовых специалистов на вакантную должность, а поиск на рынке труда кандидатов с определенными личными качествами. Когда параметры определяются по типу: «Пол неважен, образование желательно высшее, целеустремленность, коммуникабельность, умение работать самостоятельно. В настоящее время требования по многим должностям звучат именно так – как перечь общих компетентностей и умение кандидатов. Специалисты оценивают умение кандидата на основании резюме кандидата, его поведения на собеседовании, результатов тестов, анкет, заполненных кандидатом.

Но часто бывает так, что кандидат не может представить резюме, или даже если соискатель представляет резюме, то всегда стоит подвергать сомнению все, что в резюме написано, включая даже тот факт, что свое собственное резюме составлялось самим кандидатом. Анкета, заполненная кандидатом, позволяет получить информацию о его личностных характеристиках. Можно анализировать существующие анкеты кандидатов и специально формировать анкеты, чтобы определить следующие характеристики кандидатов: пунктуальность, аккуратность, исполнительность и умение работать в качестве подчиненного, внимательность, конфликтность, культурный уровень. Анкеты состоят из вопросов:

– личные данные;

– предыдущие места работы;

– умения и навыки, работа на компьютере, специализированные программы, владение языками, навыками вождения автомобиля);

– желаемый уровень заработной платы.

Специалистам по подбору кадров необходимо оценивать все документы, представленные кандидатом. Он оценивает также личностные качества кандидата.

Проверка и оценка рекомендаций кандидата. Необходимо внимательно изучать и оценить документы, предоставляемые кандидатами. В ряде случаев нестыковка в информации, полученной от работника в ходе интервью, противоречит содержанию резюме и информации в других документах. Иногда может возникнуть сомнение на предоставление кандидатом грязных документов, зачеркивания, неаккуратные записи. Важным направлением обеспечения безопасности организации является проверка рекомендаций, представленных работником. При проверке рекомендаций следует обращать внимание на странные моменты и вовремя принимать меры предосторожности.

Запрашиваемая информация должна относиться к знаниям, умениям и навыкам или другим характеристикам кандидата, необходимым для успешного выполнения работы. Акцент следует ставить на те характеристики, которые отличают эффективных работников от неэффективных. Проверка и оценка рекомендаций должна быть справедливой и обоснованной. Если система проверки рекомендаций несправедливо дискриминирует какую-либо группу или не имеет отношения к успешности выполнения работы, следует изменить эту систему или отказаться от нее. Без этого проверка рекомендаций будет не только неправомерна, но и поставит под сомнение способность организации отбирать компетентных работников. При проверке рекомендаций следует опираться на объективную информацию (биографическую или наблюдения за поведением кандидата), а не на субъективную (например, экспертная оценка личностных качеств).

У кандидатов следует запрашивать письменное разрешение на контакт с теми лицами, которые дали им рекомендации. При разговоре с лицом, давшим рекомендацию, следует выяснять, как долго он знает рекомендуемого и какую должность он занимает. Эта информация может оказаться полезной для определения обоснованности, достоверности информации, указанной в рекомендации, и выяснения того, имеет ли человек, давший ее, соответствующие полномочия на это. Вся информация, полученная в результате проверки рекомендаций, должна фиксироваться в письменном виде.

Если кандидат представил рекомендации, но эта информация не поддается проверке, попросите у кандидата дополнительные рекомендации. Зачисление в штат кандидата, не прошедшего полной проверки рекомендаций, – дело рискованное. Еще более распространены телефонные звонки предыдущему начальнику для выяснения каких-либо интересующих вопросов о его бывшем работнике. При такой проверке анализируется последовательный порядок мест работы, обращается внимание на перемены рабочих мест. При этом учитывается также частота увольнений. Считается, что у молодых работников смена рабочего места имеет другое значение. Поэтому у молодых кандидатов частые перемены рабочего места должны быть расценены положительно, так как в основе их лежат мобильность, стремление к лучшей организации, гибкость. У кандидатов постарше смена рабочего места должна быть обсуждена в ходе беседы.

Если прежние работодатели дают только общую информацию, то польза от рекомендательных писем невелика. Наиболее часто проверяемыми пунктами являются последнее место работы и образование.

Проверка данных, указанных в анкетах или резюме. Содержание анкеты в организациях устанавливается самим работодателем или агентством. При отборе на должности руководителей применяют более подробные анкеты, чем при найме простых работников.

Возможны и специальные виды анкет. Например, иногда применяют особые бланки для студентов высших учебных заведений. Поскольку трудовой стаж студентов невелик, обращают внимание на учебу, экономические способности и интересы кандидатов. В анкете запрашивается информация об учебных заведениях, специальности, объеме (в часах) курсов (каждого в отдельности), второй специальности. Запрашиваются данные об академической успеваемости кандидатов, начиная со школы: место в классе по успеваемости, средний балл, балл успеваемости в школе по дисциплинам специальности. В анкете требуется указать баллы по управленческим и юридическим дисциплинам, количество учебных часов, прослушанных по бухгалтерскому учету и анализу финансово-хозяйственной деятельности, подробные сведения об этих курсах.

Одна из задач анкетирования заключается в том, чтобы определить личностные качества и обстоятельства, которые могут помочь в работе кандидата в случае найма. Часто анкеты содержат данные о числе отработанных (за год) дней у последнего работодателя, продолжительности пропусков работы по причине болезни. Обращается особое внимание на факторы, указывающие потенциальную возможность раннего увольнения работника. В анкете запрашивается точная формулировка причин увольнения в прошлом.

Анализ анкетных данных кандидата выявляет следующее:

– соответствие уровня образования кандидата квалификационным требованиям;

– соответствие практического опыта характеру должности;

– наличие ограничений на выполнение должностных обязанностей;

– готовность к принятию дополнительных нагрузок (сверхурочные работы, командировки);

– круг лиц, которые могут рекомендовать работника, помочь наведению справок и получению дополнительной информации о кандидате.

Анализ анкетных данных наиболее распространенный метод отбора в кадровых агентствах. Агентство думает, что биография человека является надежным индикатором потенциала и полученного опыта.

Рекрутеры не придают большое значение достоверности оценки кандидата е точки зрения его психологических качеств, потенциала роста. Однако определенный уровень надежности общей оценки кандидата должен присутствовать в работе каждого агентства в зависимости от его уровня и поставленных перед ним целей и задач. Выполняя заказ клиента, кадровому агентству следует постараться свести риск представления кандидата, не соответствующего требованиям заказчика, или кандидата с плохим прошлым.

Необходимо проверять всю информацию, приведенную в анкетах и в резюме. В частности, следует проверять информацию из школы, которую закончил кандидат (подтверждение наличия грамот, медалей за успеваемость), института (наличие диплома) и с прежних мест работы (правильность указанных сроков работы, наименование занимаемой должности, исполняемые обязанности). Если при проверке обнаруживаются какие-то расхождения – это означает, что здесь требуется особое внимание.

Если результаты экспертизы документов, предоставленных кандидатом, окажутся отрицательными то данный кандидат на должность должен получить отказ от рекрутингового агентства или работодателя.

До того, как использовать полученную отрицательную информацию, следует подтвердить ее точность через другие источники. Кроме того, решения, принимаемые по разным кандидатам, должны быть последователь-

ными, то есть на основе сходной информации должны приниматься сходные решения.

Анализ анкетных данных позволяет убрать кандидатов, анкетные данные которых являются неприемлемыми для организации.

Проверка и оценка информации, указанной в характеристике кандидата. Некоторые кандидаты на должность имеют на руках характеристику с последнего места работы, если у них нет, то предприятие в праве запросить ее у бывшего работодателя (таблица 3).

Таблица 3 – Примеры формулировок, используемых в характеристиках сотрудников

№ п/п	Запись в характеристике или устное сообщение	Настоящее значение или фактическая оценка
1	…возлагаемые на данного работника задания он всегда выполнял к полному нашему удовлетворению…	Показал хорошие успехи
2	… мы были удовлетворены выполнением возлагаемых на него заданий…	Неудовлетворительная оценка
3	…он пытался решить все поставленные ему задачи…	Все его попытки не увенчались успехом
4	...он всегда старался выполнять работу с вниманием и интересом…	Усердие имело место, однако успеха не было
5	…все работы он выполнял в установленном порядке…	Он лишен собственной инициативы
6	…он действовал в меру своих способностей…	Он делал все, что было в его силах, но это было недостаточно
7	…он квалифицированный и очень добросовестный работник…	Он всегда на месте, если в нем нуждаются

Хотя характеристика и является субъективно составленным документом, тем не менее она дает специалисту по кадрам информацию о кандидате и может сыграть определенную роль в принятии им дальнейшего решения.

Система оценки кандидатов

Принятию взвешенного и обоснованного решения относительно преимущества одних кандидатов перед другими помогает использование продуманной системы оценки результатов, полученных в ходе отборочных процедур. Процедура должна быть основана на объективной информации и давать объективные оценки кандидатов; она должна помогать работникам организации, принимающим участие в процессе отбора, легче достигать

взаимопонимания при оценке кандидатов. Основой отбора выступает перечень тех качеств, которым должен удовлетворять кандидат.

В самом общем виде такими качествами являются: образовательный и профессиональный уровень, определяемый будущими должностными обязанностями (уровень образования, законченное учебное заведение, полученная специальность, общий стаж работы и стаж работы по специальности); производительность и качество труда; отношение к работе (серьезное отношение к своим обязанностям, дисциплинированность и пунктуальность, желание иметь стабильную работу); инициативность (способность ставить перед собой конкретные цели); адаптивность (умение человека адекватно реагировать на происходящие изменения и приспосабливаться к ним); готовность к сотрудничеству (умение человека эффективно выполнять совместную работу с разными людьми, эмоционально поддерживать своих коллег, своевременно вовлекая их в рабочий процесс); умение общаться (стремление понять других и быть понятым ими и умение кратко и четко формулировать и выражать свои мысли); умение решать проблемы (способность человека разбираться со сложными данными и учитывать мнение остальных людей).

В качестве отрицательных качеств кандидата выступают: отсутствие заинтересованности в делах предприятия; неопрятный внешний вид; частая смена предыдущих мест работы.

Для рекрутера при оценке кандидата на должность наиболее важными показателями являются внешний вид кандидата, его презентационные навыки, мотивации, опыт работы, образование.

Проблема безопасности при подборе персонала

Критерии отбора персонала не ограничиваются лишь теми характеристиками, которые определяют успешное выполнение работы. Важным аспектом, который в настоящее время приходится учитывать при формировании штата, является безопасность. Специально вопрос безопасности организации часто не выходит на первый план. Это не главная задача при отборе. Но при этом следует понимать, что ошибки в отборе новых работников могут являться угрозой безопасности организации из-за приема на работу человека, который умышленно или неумышленно способен нанести вред ей.

Безопасность с точки зрения организации предполагает целый ряд аспектов:

– Стремление защитить организацию от проникновения людей, имеющих связи с криминальными структурами.

– Стремление поставить барьер перед людьми, склонными к воровству. При этом чем выше должность, которую может занять такой человек,

тем больший экономический ущерб он может нанести организации, которая возьмет его на работу.

– Проверка работника на склонность к злоупотреблению алкоголем и употреблению наркотиков.

– Обеспечение информационной безопасности организации. Сюда входит не только защита секретов производства, но и защита баз данных, результатов маркетинговых исследований, планов, связанных с заключением договоров с другими организациями, и другой информации, важной для сохранения ее конкурентоспособности.

– Соответствие работника требованиям организационной культуры. Этот аспект безопасности при отборе новых работников очень недооценивается, хотя понятно, что и один человек может нанести очень большой вред организации, выражающийся в ухудшении морально-психологического климата, конфликтах, ухудшении трудовой и исполнительской дисциплины.

Существует ряд подходов, позволяющих решать проблемы безопасности при отборе сотрудников. Первый вид обеспечения безопасного подбора кадров – гарантии кадрового агентства на подбираемых работников. Эту гарантию агентство может дать не только на основании того, что методы отбора и проверки данных, представленных кандидатами, дают такую уверенность, но и потому, что многие агентства достаточно давно работают с людьми, включенными в их базу данных.

Вторым подходом является организация фирмой собственной службы безопасности для проверки кандидатов и предоставляемых ими сведений. В таких службах работают сотрудники силовых структур, обладающие соответствующими связями и возможностями. Она проверяет работника на отсутствие судимостей, отсутствие связи с криминальными структурами, отсутствие претензий предыдущих работодателей с точки зрения его честности и надежности. Проверка кандидата при приеме на работу может предполагать выяснение того, попадал ли этот человек в дорожно-транспортное происшествие, можно ли ему доверить автомобиль организации. В некоторых организациях работнику даже могут предложить принести из отделения милиции справку на себя, подтверждающую, что у него нет никаких проблем с правоохранительными органами.

УДК 004.056

Организация инфраструктуры системы защиты информации в составе информационной инфраструктуры предприятия

Е. В. Стельмашонок, д.э.н., профессор,
В. Л. Стельмашонок, к.э.н., доцент,
Санкт-Петербургский государственный экономический университет

В условиях системной нестабильности повышается зависимость национальных экономик от степени безопасности используемых информационных технологий, возникают риски информационной безопасности, связанные с ростом внешних и внутренних целенаправленных атак на бизнес-системы промышленных предприятий. В результате ключевые бизнес-процессы промышленных предприятий подвергаются негативным воздействиям: остановка или прерывание функционирования систем и сервисов; повреждение, потеря или компрометация данных; прямые финансовые потери в результате противоправных действий киберпреступников.

Анализ динамики атак и потенциальных угроз информационной безопасности [1] показал, что разработка систем управления информационной безопасностью имеет стратегическое значение для развития национальной экономики России.

В процессе перехода к цифровой экономике и необходимости защиты критической информационной инфраструктуры повышаются требования к безопасности информационных технологий, обеспечивающих функционирование бизнес-процессов промышленных предприятий.

Информационная инфраструктура предприятия должна обеспечивать безопасную обработку данных и информационное сопровождение бизнес-процессов внутри промышленного предприятия, а также обмен информационными ресурсами с внешней средой, что соответствует цели непрерывности бизнеса.

Под информационной инфраструктурой понимается набор типовых технологических элементов, инструментария и методик, которые, с одной стороны, не зависят от конкретной решаемой задачи, а с другой стороны, легко стыкуются между собой и имеют средства интеграции с существующими «унаследованными» подсистемами [2]. Информационная инфраструктура промышленного предприятия позволяет обеспечить надежное функционирование и взаимодействие всех входящих в информационную систему функциональных модулей и прикладных подсистем, представить комплекс необходимых средств и инструментов для управления системой, ее сопровождения и развития.

В рамках информационной инфраструктуры промышленного предприятия необходимо создать четко работающую инфраструктуру защиты информации бизнес-процессов, необходимую для обеспечения непрерывности бизнес-процессов предприятия. На рисунке 1 представлена инфраструктура системы защиты информации бизнес-процессов промышленного предприятия, механизм взаимодействия элементов этой системы: защита от несанкционированного доступа, от перехвата при передаче информации, от случайных помех и сбоев, от информационного вмешательства в бизнес-процесс [3].

Управление информационными рисками является частью общей системы менеджмента, которая основана на процессно-ориентированном подходе при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности промышленного предприятия.

Внедрение системы управления информационной безопасностью направлено на систематическую идентификацию, анализ и смягчение рисков информационной безопасности, рисков, в результате которых информационные активы подвергаются нарушению конфиденциальности, целостности и доступности.

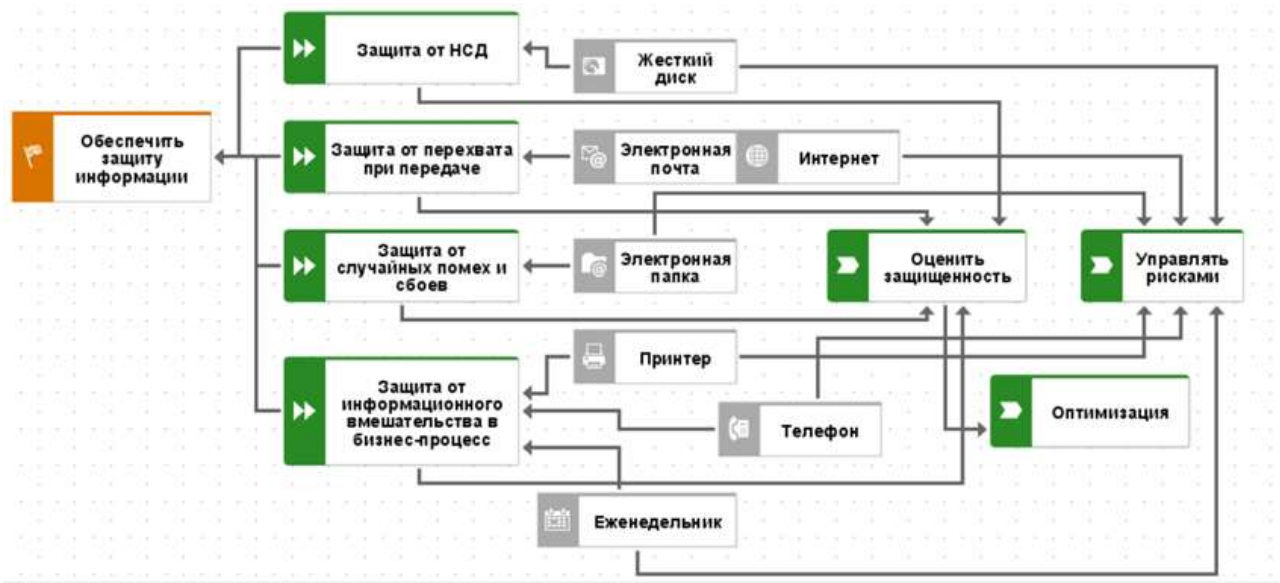

Рисунок 1 – Инфраструктура системы защиты информации бизнес-процессов на промышленном предприятии

Защита информационных ресурсов, прежде всего, направлена против различного вида угроз. Информационным ресурсам могут грозить [4]:

– несанкционированный доступ к конфиденциальным данным как извне, так и изнутри структуры, их корыстное использование и разглашение;

– перехват, подмена и искажение информации в процессе передачи;

– целенаправленное искажение, фальсификация или подмена данных при несанкционированном доступе;

– информационное вмешательство в бизнес-процесс.

В системе управления информационной безопасностью промышленного предприятия малоисследованной и требующей отдельного рассмотрения является система управления рисками.

Процесс управления рисками информационной безопасности включает следующие этапы, представленные на рисунке 2: планирование, реализацию, проверку, совершенствование и выполнение следующих процедур:

– выбор объектов защиты;
– выбор методологии оценки рисков;
– идентификация активов;
– анализ угроз и их последствий;
– обработка рисков;
– выбор защитных мер;
– переоценка и оценка остаточного риска.

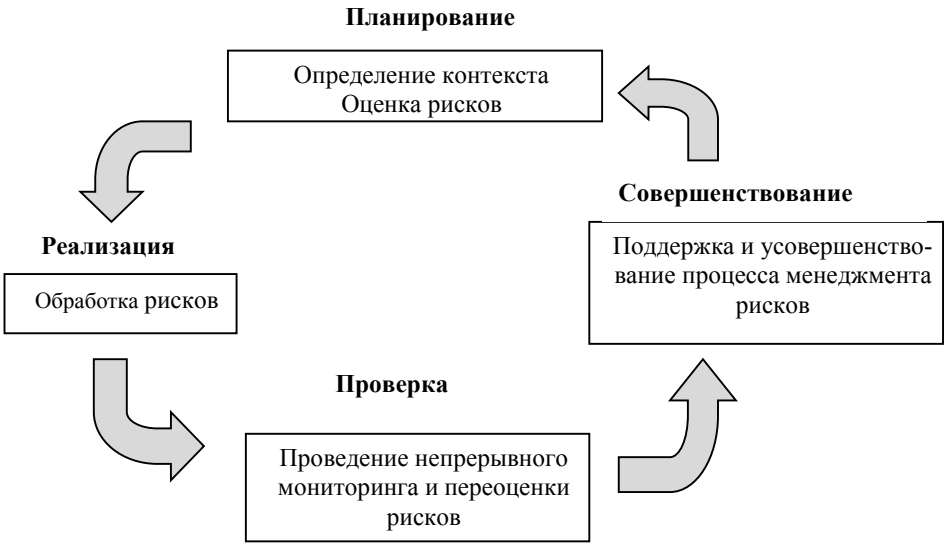

Рисунок 2 – Процесс управления рисками информационной безопасности

Критерии оценки рисков информационной безопасности должны учитывать стратегическую ценность информационных активов, защищенность информации с позиции конфиденциальности, целостности и доступности. На этапе планирования определение *контекста* заключается в формулировании цели менеджмента рисков информационной безопасности, разработке критериев принятия риска и определении допустимых уровней риска [5].

Кроме того, при определении контекста предприятие должно оценить, имеются ли необходимые ресурсы для:

– выполнения оценки рисков и создания плана по обработки рисков;

– определения и реализации политик и процедур, включая реализацию выбранных мер и средств контроля и управления;

– осуществления мониторинга мер и средств контроля и управления;

– осуществления мониторинга процесса менеджмента рисков информационной безопасности.

При этом анализируются:

– классификационный уровень информационного актива в зоне риска;

– наиболее вероятные угрозы нарушения информационной безопасности (целостности, доступности и конфиденциальности, оперативной деятельности промышленного предприятия);

– оцениваются финансовые потери, предполагаемый ущерб для репутации.

Под *принятием риска* понимается решение о допустимости существующего уровня риска, то есть промышленное предприятие допускает вероятность наступления возможных негативных последствий.

При этом необходимо учитывать следующее:

– критерии принятия риска могут включать ряд пороговых значений, когда указывается желаемый целевой уровень риска, при оговорке, что при определенных обстоятельствах высшее руководство будет принимать риски, находящиеся выше этого уровня;

– критерии принятия риска могут выражаться как соотношение количественно оцененной прибыли (или иной выгоды для бизнеса) и количественно оцененного риска;

– к различным классам рисков могут применяться разные критерии принятия рисков. Например, могут не приниматься риски, связанные с требованием законодательства, в тоже время может допускаться принятие рисков высокого уровня, если это определено договорными обязательствами;

– критерии принятия риска могут включать требования по дополнительной обработке риска в дальнейшем. Например, риск может быть принят, если взяты обязательства принять меры по снижению уровня риска в течение определенного периода времени;

– критерии принятия риска могут различаться и в зависимости от того, насколько долго предположительно риск будет существовать, например, он связан с кратковременной или долговременной деятельностью;

– критерии принятия риска устанавливаются с учетом критериев бизнеса, особенностей законодательства, операций, технологий, финансов, социальных и гуманитарных факторов.

Оценка рисков – общий процесс анализа рисков и их оценивания представлен на рисунке 3.

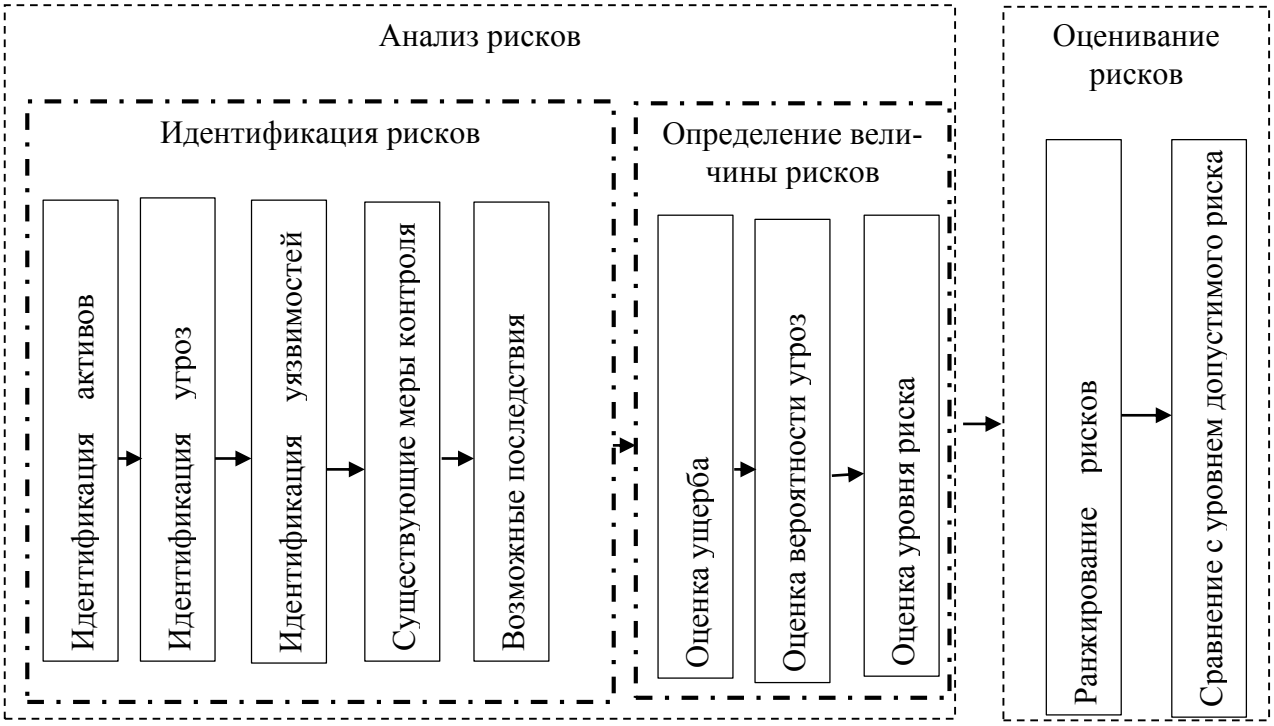

Рисунок 3 – Основные этапы оценки рисков

Анализ рисков – систематическое использование информации для определения источников риска и определения его величины.

Анализ рисков состоит из процедур:

– идентификации рисков, включающую идентификацию активов, угроз этим активам, уязвимости активов, которые могут быть использованы угрозами, существующие меры контроля и возможные последствия воздействия на активы в результате реализации угроз информационной безопасности;

– определения величины (уровня) рисков – подразумевает присвоение значений вероятности и последствиям риска.

На этом этапе оценивается:

– ущерб (негативные последствия) для основной деятельности предприятия, который может быть нанесен в результате возможной реализации угроз ИБ;

– вероятность реализации угроз с учетом существующих уязвимостей активов и применяемых мер защиты информации;

– уровни рисков.

Информационным ресурсам могут грозить:

– приведение систем передачи информации в неработоспособное состояние в результате злонамеренных или неосторожных действий, например, путем перегрузки бесполезной информацией («спам»);

– несанкционированный доступ к конфиденциальным данным как извне, так и изнутри структуры, их корыстное использование и разглашение;

– целенаправленное искажение, фальсификация или подмена данных при несанкционированном доступе;

– подмена и искажение информации, предоставленной для свободного доступа.

Поддержание устойчивости системы управления промышленным предприятием невозможно без оценки защищенности бизнес-процессов промышленных предприятий.

Задача оптимизации инфраструктуры защиты информации промышленного предприятия может быть формализована в виде комплекса математических моделей, включающих:

– модель минимизации затрат на оптимизацию инфраструктуры защиты информации;

– модель максимизации уровень качества инфраструктуры защиты информации [4].

Целесообразно совместное использование этих моделей. Так, при ограничении на допустимые затраты на защиту может быть найдено максимальное значение качества инфраструктуры защиты информации. В некоторых случаях эта задача может иметь не одно, а несколько решений (профилей защиты). Для выбора того решения, из числа найденных оптимальных решений, которое требует минимальных затрат на защиту, следует решить вторую задачу. В ней в качестве ограничения должно присутствовать найденное в первой задаче значение качества инфраструктуры защиты информации.

Оптимальная по стоимости система защиты информации при этом не является самой безопасной.

Концепция экономически оптимальной системы защиты информации имеет ограниченное применение. Возможна ситуация, когда не зависимо от стоимости системы защиты информации вероятность нанесения ущерба остается постоянной или даже является положительной величиной (в связи с ростом уязвимости самой системы защиты информации). В последнем случае встает вопрос об отказе от системы защиты информации.

Список литературы

1. Positive Technologies. Аналитика [сайт]. URL: https://www.ptsecurity.com/ru-ru/research/analytics (дата обращения: 09.11.19).
2. Стельмашонок Е.В., Еникеева Л.А. Управление информационными рисками как основа устойчивого развития компании. Научно-технические ведомости СПбГТУ, №1, 2006. – С. 146-149.
3. Стельмашонок Е.В., Тарзанов В.В., Стельмашонок В.Л. Моделирование коррелированных угроз информационной безопасности предприятия. Вестник ИНЖЭКОНа, вып. №5(48) серия «Экономика», – СПб.: СПбГИЭУ, 2011. – с.175-181.

4. Стельмашонок Е.В. Организация информационной защиты бизнес-процессов // Прикладная информатика. 2006. № 2. – С. 42–57.
5. Безопасность современных информационных технологий: Монография / Е.В. Стельмашонок [и др.]; под общей редакцией Е.В. Стельмашонок. СПб.: СПбГИЭУ, 2012. – 408 с.

УДК 004.021, 004.056.5

Особенности разработки методов и моделирования информационной защищенности оператора автоматизированных систем

В. В. Сухостат, к.т.н., к.п.н., доцент,
Санкт-Петербургский государственный экономический университет,
СЗИУ РАНХиГС при Президенте РФ

Существенными особенностями нынешнего момента можно обозначить сингулярности следующего порядка:

– экспоненциальные темпы развития новых технологий и комплексный характер их воздействия на все сферы человеческой деятельности (экономика, промышленность, обороноспособность, наука, образование, культура, бизнес, социальная сфера);

– новые цифровые технологии обнаруживают беспрецедентное влияние на развитие каждой отдельной личности (интеллектуальное, эмоциональное, нравственное);

– противоречивый характер, т.к. новые цифровые технологии – это большие возможности для развития и одновременно огромные потенциальные угрозы и риски [6].

Это влечет за собой постоянное повышение сложности и увеличение масштабности деструктивных воздействий на объекты критической информационной инфраструктуры. Поэтому жизненно важной задачей становится максимальная защищенность автоматизированных систем от киберугроз [7]. В этой связи следует отметить особенности разработки методов и моделей информационной защищенности оператора автоматизированных систем.

С точки зрения связи информационной защищенности оператора автоматизированных систем с его психофизиологическим состоянием как меры информационной защищенности характеристика информационной системы, в частности человека-оператора, может быть использована нарушителем с целью реализации угроз [3]. В связи с этим возникает вопрос рассмотрения сущностных характеристик оператора в информационной системе, его информационной модели.

Анализ теоретических и эмпирических исследований в области инженерной психологии и эргономики, управления в социальных и экономических системах [5, 10-12] свидетельствует, что эффективность деятельности человека-оператора обеспечивается совокупностью функциональных, психологических процессов и свойств личности. Поэтому для сложной информационно-энергетической системы, которой является человеческий организм, получение оценки защищенности оператора требует комплексного подхода, который может быть реализован путем интеграции отдельных показателей состояния функциональных систем в оценку психофизиологического состояния.

В этой связи, диагностические процедуры и алгоритмы прогноза успешности его деятельности должны учитывать профессионально-личностные качества человека как объекта защиты и объекта обеспечения информационно-психологической безопасности информационных систем.

В этом случае оценка психофизиологического состояния получается как взвешенная свертка совокупности его информативных показателей с последующей обработкой полученных результатов.

Также, для выявления и определения нового вида угроз для оператора сегодня необходимо исходить из того, что биоинформационный процесс в организме зависит не от интенсивности электромагнитных волн, а от их информационного содержания: частоты, модуляции, поляризации и т.п. [1]. Поэтому, чтобы выявить характер информационно-психологических воздействий на организм, надо рассмотреть информационную модель оператора.

С точки зрения психодиагностики человека можно представить в виде совокупности различных психофизиологических характеристик. Используя количественную оценку этих характеристик по стандартизованной шкале, можно получить определенную оценку его поведения в различных ситуациях.

Так, в [8] предложен перечень психофизиологических характеристик, условно разделенных на три части: психологические, физиологические и контролирующие характеристики.

К физиологическим характеристикам относятся зрение, слух, обоняние, осязание, речь, нервная система. Психологические характеристики – внимание, память, воображение, мышление, темперамент, характер, воля, эмоции, личностные характеристики, мотивация, уровень интеллекта. Показатели для контролирующих систем: уровень знаний, специальные навыки, степень освоения теоретического материала, оценка знаний, степень освоения практического материала.

Вопрос об оценке психофизиологического состояния человека находит свое решение при использовании выше указанного набора признаков [2, 8], которые можно представить в виде информационной

модели человека-оператора, представленной на рисунке 1. Кардинальные составляющие этой модели нуждаются в кратком пояснении. Прежде всего, следует подчеркнуть комплексный подход к исследованию оператора, так как отдельные показатели состояния функциональных систем организма могут быть интегрированы в оценку психофизиологического состояния.

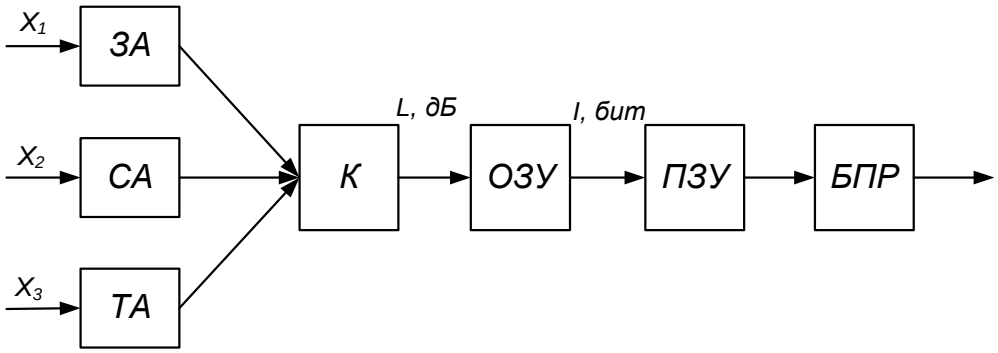

Рисунок 1 – Схема информационной модели человека,
где ЗА – зрительный анализатор, СА – слуховой анализатор, ТА – тактильный анализатор, К – коммутатор, ОЗУ – оперативное запоминающее устройство, ПЗУ – постоянное запоминающее устройство, БПР – блок принятия решений [8]

На уровне физиологии у человека можно выделить следующие основные блоки:

– зрительный анализатор,
– слуховой анализатор,
– тактильный анализатор,
– коммутатор.

Через эти блоки происходит прием и преобразование входных сигналов во внутренние ощущения человека. Этот уровень обеспечивает безопасность жизнедеятельности, ориентировки и перемещения человека в окружающем мире [8].

Ощущения человека рассматриваются как основные физиологические характеристики, функции которых состоят в преобразовании внешних сигналов в количественные и качественные показатели приема, усвоения информации человеком и управляющие движения для обеспечения взаимодействия человека со средой [2, 8].

На уровне психологии человека можно выделить следующие модули:

– оперативное запоминающее устройство;
– постоянное запоминающее устройство;
– модуль принятия решения.

Они позволяют решать стратегические задачи, определять цели и направления деятельности человека при минимальном риске, обеспечивают устойчивость и надежность ожидаемого поведения человека.

С помощью анализаторов человеку поступает первичная информация о состоянии внешней среды и автоматизированной системы. Процесс приема и первичной переработки этой информации называется сенсорным восприятием, а сама информация – сенсорной (ощущением).

Ощущение – информация об отдельных свойствах или явлениях материального мира, а также внутренних состояний организма, получаемая при непосредственном воздействии раздражителей на соответствующие рецепторы.

В зависимости от специфики принимаемых сигналов различают анализаторы:

– зрительный;

– слуховой;

– тактильный, болевой, температурный;

– обонятельный;

– вкусовой;

– внутренние: давления, кинестетический, вестибулярный, специальные, расположенные во внутренних органах и полостях тела.

С точки зрения эргатической системы считается, что до 80% всей информации человеку поступает через зрительный анализатор, около 19% – через слуховой и только 1% – через тактильный.

Различают следующие основные параметры анализаторов [8, 10]:

– абсолютная чувствительность – минимальное значение раздражителя, вызывающего начальные ощущения;

– предельно допустимая интенсивность сигнала – болевой порог восприятия;

– диапазон чувствительности – зона восприятия сигнала от абсолютного до болевого порога;

– дифференциальная чувствительность – минимальное изменение интенсивности сигнала, ощущаемое человеком;

– границы спектральной чувствительности – абсолютные пороги ощущений по частоте сигнала;

– дифференциальная чувствительность к изменению частоты сигнала – дифференциальный, различительный порог по частоте.

Рецепторы человека обладают следующей специфической особенностью: у них большой диапазон значений интенсивности сигналов, в пределах которого возможно эффективное функционирование анализаторов, при высокой дифференциальной чувствительностью к интенсивности. Такое свойство оказывается допустимым благодаря системе адаптации и возмож-

ности понижать или повышать чувствительность анализаторов в зависимости от средней интенсивности сигналов, воздействующих в течение определенного времени.

Зрительный анализатор. Человеческий глаз как система непосредственного визуального наблюдения является способом регистрации оптического сигнала. На внутренней поверхности глаза (на его сетчатке) образуется оптическое изображение, воспринимаемое человеком как зрительный образ [2, 4].

Свет, делающий для глаза окружающий мир видимым, по современным воззрениям представляет единство волнового и квантового процессов. Связь волновой характеристики света (длины волны λ) и его квантовой характеристики (массы фотона $m_ф$) для вакуума описывается равенством:

$$\lambda = \frac{c}{v_b} = \frac{h_П}{m_ф \cdot c}$$

где $h_П$ – постоянная Планка, $v_в$ – частота электромагнитной волны, c – скорость света в вакууме. При этом энергия $\varepsilon_ф$ фотона (кванта) определяется по формуле:

$$\varepsilon_ф = h_П \cdot v_b = m_ф \cdot c^2$$

Таким образом, квантовому характеру движения фотонов соответствует волновой процесс с частотой $v_в$, причем скорость движения фотонов (квантов) в вакууме такая же, как скорость распространения в вакууме электрических волн, и приблизительно эта скорость (т.е. скорость распространения света) равна с ≈ 300 000 км/с = $3 \cdot 10^8$ м/с.

Здесь целесообразно отметить, что скорость света только в вакууме не зависит от длины волны. В любой другой среде зависит от длины волны λ. Частота $v_в$ остается постоянной в разных изотропных средах, т.е. средах, физические свойства которых одинаковы по всем выбранным в них направлениях.

Вышеприведенные соотношения позволяют оценить чувствительность глаза $U_{(г)}$ в квантах за 1 с, так как нормальный глаз человека способен реагировать на очень малые потоки энергии $P_{min(г)} = 3 \cdot 10^{-10}$эрг/с.

Световая энергия является материальным носителем зрительных ощущений. Световой диапазон, в котором зрительный анализатор принимает и анализирует информацию, составляет 380–780 нм.

В сетчатке имеется участок, так называемое, «слепое пятно». В этом участке отсутствуют чувствительные элементы, и сетчатка на этом участке не обладает чувствительностью к свету.

Относительные изменения интенсивности, к которой глаз может приспосабливаться, превышают 1 млн. раз. Это свойство позволяет глазу адаптироваться к внешнему световому воздействию.

В сетчатке происходит предварительная обработка информации на уровне зрительного анализатора. Дальнейшую обработку сигналов проводит зрительный корковый центр [8].

Известен закон Вебера-Фехнера, которому подчиняется психофизиологическое восприятие освещенности E зрительным анализатором человека: прирост ощущений пропорционален логарифму отношения энергий сравниваемых раздражений:

$$L = \lg(\frac{E}{E_0}),$$

где L – световые ощущения человека; E – освещенность объекта, E_0 – порог восприятия освещенности зрительным анализатором человека.

Вместе с тем, глаз, работающий совместно с оптическими приборами, налагает определенные ограничения на рабочий диапазон длин волн. При этом на всей протяженной области длин волн оптического излучения (от 1 нм до 1 мм) условно принято различать:

– видимое излучение, которое воспринимается глазом и способное непосредственно вызывать зрительное ощущение в диапазоне длин волн от 380 нм до 780 нм;

– инфракрасное излучение (невоспринимаемое глазом), длины волн которого удовлетворяют двойному неравенству 780нм<ИК<10^6нм, где ИК – инфракрасное излучение;

– ультрафиолетовое излучение (невоспринимаемое глазом), длины волн которого больше 1нм и меньше 380нм, т.е. 1нм<УФ<380нм, где УФ – ультрафиолетовое излучение.

Соотношение субъективной оценки цвета с длиной волны составляют для фиолетового цвета 380–420 нм; синего – 450–480 нм; голубого – 480–510 нм; зеленого – 510–550 нм; желтого – 575–585 нм; оранжевого – 585–620 нм; красного – 620–780 нм [2, 4, 10].

Спектральная чувствительность глаза к частотному спектру сигнала неодинакова. В дневное время суток наибольшая чувствительность зрения проявляется к излучению с длиной волны 555 нм (желто-зеленый цвет) и уменьшается к границам видимого спектра, а в ночное время суток эта характеристика смещается в область фиолетового спектра. С помощью параболического закона можно описать зависимость чувствительности зрительного анализатора от спектрального состава света

$$L_f = k \cdot f^2,$$

где k – коэффициент пропорциональности; f – частотная характеристика света, Гц.

Максимальная чувствительность зрительного анализатора в дневное время суток лежит в зеленом спектре частот, а в ночное время смещается в ультрафиолетовую область. Ультрафиолетовое излучение перекрывается рентгеновским, а инфракрасное – радиоволнами.

Слуховой анализатор. Одним из существенных физических аспектов информационно-полевых угроз является звук. Понятие звука ассоциируется со слухом и, следовательно, с физиологическими процессами в ушах, а также с психофизиологическими процессами в мозгу (там происходит переработка ощущений, поступающих в органы слуха). Применительно к восприятию акустической информации следует отметить предельные возможности органа слуха, чувствительность которого превосходит во многих отношениях свойства лучшей акустической техники [4, 8].

Слуховой анализатор является одним из важнейших информационных каналов человека и состоит из периферической части (собственно уха), проводниковой части (волокон слухового нерва вместе с проводящими путями мозга) и центральной части (височной области коры больших полушарий головного мозга) [4]. Собственно ухо включает в себя наружное ухо, среднее ухо и внутреннее ухо. Между наружным и средним ухом находится передающая звуковые сигналы перепонка – упругая, тонкая (≈ 0,1 мм) соединительная пластинка, работающая как приемник давления.

В отличие от зрительного анализатора, который требует направленности и сосредоточенности человека на объект исследования, слуховой анализатор не требует подобного сосредоточения. По слуховому каналу действуют также шумы, которые являются источниками помех для прохождения информации человеку. Носителем слуховых ощущений является звуковая энергия.

Звук воспринимается человеком с помощью чувствительного психофизиологического отражения как двухмерное пространство в координатах интенсивности звука I и частоты f, которое переводится в его субъективные ощущения – уровень звукового давления или уровень громкости L (дБ), который подчиняется психофизиологическому закону Вебера–Фехнера:

$$L = 10\lg\frac{I}{I_0},$$

где I и I_0 (10^{-12} Вт/м^2) – текущая интенсивность звука и порог слышимости звука человеком соответственно.

Болевой порог составляет $I_{бп}$ = 10 Вт/м^2. Уровень громкости болевого порога равен $L_{бп}$ =10 lg 10^{13} = 130 (дБ).

Таким образом, информационный интервал восприятия интенсивности звука человеком составляет 0-130 дБ (от 10^{-12} до 10 Вт/м^2). Слуховой анализатор человека воспринимает частотный диапазон в пределах 20-20000 Гц.

Субъективное восприятие частоты звука L_f человеком при постоянном значении интенсивности звука также подчиняется психофизиологическому закону Вебера–Фехнера [8]:

$$L_f = \log_2 \frac{f_в}{f_н},$$

где $f_в$ и $f_н$ – верхняя и нижняя граничные частоты интервала соответственно, Гц.

Верхняя граничная частота $f_в$ октавы определяется путем удвоения нижней граничной частоты: $f_в = 2 f_н$.

Каждую октаву принято обозначать среднегеометрической частотой, которая может быть найдена как

$$f_{ср} = \sqrt{f_в \, f_н} = f_н\sqrt{2} \quad .$$

Условно весь звуковой спектр частот разбит на 9 октавных полос со следующими среднегеометрическими частотами [9]:

Номер октавы	*I*	*II*	*III*	*IV*	*V*	*VI*	*VII*	*VIII*	*IX*
$f_{ср}$, Гц	*31,5*	*63*	*125*	*250*	*500*	*1000*	*2000*	*4000*	*8000*

Нижняя граничная частота *I* октавы составляет 31,5 Гц, а верхняя граничная частота *IX* октавы составляет 11 200Гц.

Таким образом, условно считается, что слышимый человеком звуковой частотный диапазон составляет порядка 22,3-11200 Гц. Звуки, которые лежат в диапазоне ниже 22,3 Гц, называются *инфразвуками*, а звуки с частотой спектра более 11 200 Гц – *ультразвуками*.

Восприятие высоты звуковых сигналов в основном обусловлено их частотными характеристиками. Однако ощущение в некоторой степени зависит также от силы звукового раздражителя и состава звука. С увеличением уровня громкости ощущение высоты тона низких частот несколько понижается, высоких – возрастает. В среднем диапазоне частот (1000–2000 Гц) ощущение высоты практически не зависит от громкости.

Дифференциальная чувствительность к изменению высоты тона определяется константой Вебера $k = \frac{\Delta f}{f}$. В диапазоне частот 500-5000 Гц при средних уровнях интенсивности величина k = 0,002…003.

Дифференциальная чувствительность возрастает с ростом интенсивности звука.

Временной порог t обнаружения звуковых сигналов связан с абсолютным порогом слышимости. В диапазоне (5-20) < t < (100-200) мс действует закономерность $(I - I_0)\ t$ = const, где I_0 – подпороговая интенсивность, максимально близкая к порогу, но не вызывающая слухового ощущения ни при каких условиях.

При t < 10 мс порог слышимости круто повышается в сторону малых длительностей. В средней области частот порог слышимости при t = 0,5 мс на 20-22 дБ выше порога при t = 220 мс. Аналогично при переходе от t_1 = = 1 мс к t_2 = 1 с порог слышимости снижается на 22-24 дБ. Временной порог различения интервалов между звуками составляет 0,5-2 мс. Пороговое время опознания прерывистых тональных звуковых сигналов (интервал дискретности) составляет $t_{кр}$ = 80-150 мс. При $t < t_{кр}$ информация о сигнале обрабатывается слуховым анализатором не полностью:

− при t = 20-40 мс два следующих один за другим коротких тональных сигнала воспринимаются как один неоднородный сигнал;

− при t = 40-80 мс те же сигналы воспринимаются как два, в какой-то мере влияющие друг на друга, но в то же время имеющие неразличимые индивидуальные характеристики.

Минимальное время восприятия высоты тонов в средней области частот при L = 80 дБ соответствует 10-12 периодам; грубое восприятие возможно при 6-8 периодах. При снижении интенсивности до 40 дБ временной порог опознавания высоты увеличивается в 1,5-2,5 раза (для 1000 Гц – с 10 до 22 мс, для 125 Гц – с 24 до 40 мс). Для опознания высоты тона необходимо обеспечить не менее 90-110 мс [4, 8].

Пространственная локализация источника звука возможна благодаря восприятию звуков одновременно двумя ушами (бинауральный слух). *Бинауральный слух* от моноурального отличается более высокой абсолютной чувствительностью, помехоустойчивостью, разрешающей способностью при дифференцировании изменений высоты и громкости тональных сигналов и большей возможностью различения пространственного расположения источника звука.

Пространственная локализация источников звука осуществляется благодаря:

– разнице во времени прихода сигналов на правое и левое ухо (интервал в 30-40 мс создает впечатление смещения источника на 2-3° в сторону уха, в которое сигнал приходит раньше);

– сдвигу фазы сигналов, поступающих на разные уши. Бинауральная фазовая чувствительность наиболее выражена для диапазона f = 200-250 Гц, в сторону более высоких и более низких частот она ухудшается, при 2000-3000 Гц практически отсутствует. Разность фаз 180° соответствует смещению источника звука на 90°;

– разнице интенсивности сигналов, приходящих к правому и левому уху.

В определении направления на источник звука при f = 1000 Гц преобладающую роль играет запаздывание и фазовый сдвиг сигнала, при $f > 4000$ Гц – разница в громкости, при 1000 < f < 4000 Гц работают оба механизма.

Диапазоны частот f = 100-8000 Гц и интенсивности звука I = 0-65 дБ характеризуют основные речевые звуки. От соотношения уровней шума и речи зависит влияние шума на разборчивость звуковых сигналов. Удовлетворительное восприятие речи должно соответствовать уровню, не превышающему шум на 6 дБ.

Темп речи 60-80 слов в 1 мин с интервалом между словами 1с считается оптимальным, а допустимым – до 120 слов в 1 мин.

Кожный анализатор обеспечивает восприятие прикосновения (слабого давления), боли, тепла, холода и вибрации [9]. Для каждого из этих ощущений (кроме вибрации) в коже имеются специфические рецепторы, либо их роль выполняют свободные нервные окончания. Каждый участок кожи обладает наибольшей чувствительностью к тем раздражителям, для которых на этом участке имеется наибольшая концентрация соответствующих рецепторов, поэтому можно выделить на коже точки и участки с избирательной чувствительностью к прикосновению, боли, теплу, холоду. При ритмичных последовательных прикосновениях к коже каждое из них воспринимается как раздельное, пока не будет достигнута *критическая частота* $f_{кр}$, при которой ощущение последовательных прикосновений переходит в специфическое ощущение *вибрации.* В зависимости от условий и места раздражения $f_{кр}$ = 5-20 Гц.

При $f = f_{кр}$ тактильная чувствительность переходит в вибрационную.

Вибрационная чувствительность обусловливается теми же рецепторами, что и тактильная, поэтому топография распределения вибрационной чувствительности по поверхности тела аналогична тактильной.

Кинетическая энергия вибрации воспринимается органами чувств человека по закону Вебера-Фехнера. Она равна:

$$L = 10\lg\frac{W}{W_0} = 10\lg\frac{\frac{mV^2}{2}}{\frac{mV_0^2}{2}} = 10\lg\frac{mV^2}{mV_0^2} = 10\lg\frac{V^2}{V_0^2} = 20\lg\frac{V}{V_0}\ (\text{дБ}),$$

где $W = \frac{mV^2}{2}$ – текущее значение кинетической энергии вибрации; $W_0 = \frac{mV_0^2}{2}$ – порог восприятия кинетической энергии человеком; m – масса человека; V – текущее значение виброскорости; $V_0 = 5 \cdot 10^{-8}$ *м/с* – пороговое значение виброскорости, воспринимаемое человеком.

Одновременное изменение виброскорости и частоты оценивается человеком по известному закону параболы $L = k \cdot f^2$, где k – коэффициент пропорциональности.

Структурную модель психологии человека может быть представлена в виде блоков оперативной и постоянной памяти, блока принятия решений.

Память человека включает процессы запоминания, хранения, узнавания, понимания и воспроизведения информации.

Различают следующие виды памяти [5, 8, 11]:

– *двигательная* (*моторная*) *память*, которая обеспечивает запоминание, воспроизведение движений и их комбинаций, лежащих в основе выработки и формирования двигательных навыков и привычек;

– *эмоциональная память* – память человека на пережитые им в прошлом чувства;

– *образная память* обеспечивает сохранение и воспроизведение образов ранее воспринимавшихся предметов и явлений;

– *эйдетическая память* – очень ярко выраженная образная память, связанная с наличием ярких, четких, живых, наглядных представлений;

– *словесно-логическая память* обеспечивает запоминание и воспроизведение мыслей, текста, речи.

Память человека бывает непроизвольной и произвольной. *Непроизвольная память* проявляется в тех случаях, когда тот или иной материал запоминается без применения специальных приемов и усилий. *Произвольная память* связана с целью запоминания того или иного материала, применением специальных приемов и волевых усилий человека.

По объему, функциональному назначению и длительности сохранения информации различают оперативную (кратковременную) и постоянную (долговременную) память. *Оперативная память* характеризуется кратковременностью процессов (запоминания, хранения и воспроизведения информации), актуальностью действий человека. Для *постоянной памяти* характерно длительное сохранение материала после многократного его повторения и воспроизведения.

Оперативная память позволяет сохранять текущую информацию на время, необходимое для решения конкретных практических задач. В зависимости от вида деятельности это время в реальных условиях изменяется от нескольких секунд до нескольких минут. Объем оперативной памяти почти не зависит от информационного содержания материала и определяется

количеством запоминаемых символов. Оперативная память выполняет функцию кратковременной памяти с небольшой емкостью и высокой скоростью обработки, способную принимать и удерживать входную информацию. Вновь поступающий в память символ вытесняет оттуда один из поступивших ранее, если он не перешел к тому времени в долговременную память.

Пропускную способность системы определяют скорость запоминания и воспроизведения информации оперативной памятью. В случае, когда поступающая информация не превышает объем оперативной памяти, скорость приема информации составляет несколько бит/с. Но, если объем информации превышает емкость оперативной памяти, скорость запоминания резко снижается до десятых долей бит/с и даже менее.

Факторами функционирования оперативной памяти являются:

– система кодирования информации (для оперативного запоминания предпочтительно кодирование объектов цифрами и буквами);

– структурирование информации;

– порядок представления информации (предпочтительно одновременное предъявление сведений);

– систематизация информации в процессе запоминания.

Немаловажной характеристикой оперативной памяти является быстрота забывания информации, которая не понадобится в процессе деятельности. Своевременность забывания исключает ошибки, связанные с использованием устаревшей информации, тем самым освобождает место для хранения новых данных.

Хранение информации в течение длительного времени обеспечивается долговременной памятью. Ее объем ограничен количеством сохраняемой информации, и составляет около 10^{20} бит. Скорость обработки информации долговременной памятью составляет порядка $0{,}1 \le V \le 10$ бит/с.

Оперативная память связана с первичной ориентировкой человека в окружающей среде, она фиксирует общее число внешних сигналов независимо от их информационного содержания, а задачей долговременной памяти является организация поведения человека в будущем.

Процесс перевода данных из оперативной в долговременную память заключается в преобразовании сообщения, направленного на выделение смыслового содержания, исключению лишней информации, мешающей запоминанию. В то же время избыточная информация, не создавая дополнительной нагрузки на память, облегчает запоминание, что эквивалентно увеличению объема долговременной памяти. Процесс перевода информации из кратковременной в долговременную память может не требовать специальных усилий и осуществляться непроизвольно, но может быть и произвольным, требующим специальных действий и волевых усилий.

Составляющими психологического процесса функционирования памяти человека являются [5, 12]:

– *запоминание* – процесс закрепления в сознании образов, впечатлений, понятий;

– *узнавание* – процесс в памяти, связанный с осознанием того, что данный объект воспринимался в прошлом;

– *забывание* – процесс, при котором происходит «выпадение» того или иного материала из памяти;

– *воспроизведение* – процесс извлечения информации из памяти;

– *ассоциация* – связь между отдельными представлениями, при которых одно представление вызывает другое;

– *представления* – образы предметов или процессов реальной действительности, в данный момент не воспринимаемых человеком.

Принятие решений является важнейшим компонентом операторской деятельности. Любое решение оператора является результатом приема и переработки информации. Однако, в зависимости от назначения АС, психологические механизмы, предшествующие выработке решения, существенно различаются.

Процесс принятия решения включает: формулирование проблемы, генерацию вариантов решения (гипотез), оценку вариантов по выбранным критериям, выбор того варианта решения, который максимально обеспечивает достижение цели.

Функциями блока принятия решений являются функции мышления, анализа, синтеза, обобщения, воображения. *Мышление* – процесс обобщенного и опосредствованного познания свойств и явлений окружающей действительности, а также связей и отношений, существующих между ними [2, 3, 5, 7, 8, 10]. Мышление делится на абстрактное и конкретное мышление. Абстрактное мышление опирается на общие и отвлеченные понятия. Конкретное мышление – умственная операция, в процессе которой человек придает предметный характер той или иной абстрактно-обобщенной мысли, понятию, правилу, закону.

Анализ – мысленное расчленение предметов и явлений на образующие их части, выделение в них отдельных частей, признаков, свойств.

Синтез – мысленное соединение отдельных элементов, частей и признаков в единое целое. *Обобщение* – операция, состоящая в мысленном объединении предметов или явлений по общим и существенным признакам.

Воображение – процесс создания образов – представлений нового. Непроизвольное (пассивное) воображение возникает без всякого намерения со стороны человека. Произвольное (активное) воображение возникает в результате поставленной человеком цели, намерения.

На уровне блока принятия решений идет осмысление полученного внешнего сигнала человеком, вырабатываются решения стратегического характера для его деятельности в будущем. На этом уровне осуществляется преобразование ощущений человека L в информацию I, т.е. осуществляется переход от материального к психологическому.

Американский ученый Хик в своем законе показал, что время реакции $T_р$ человека на входную информацию I зависит не только от ее количества, но и качества (смысла):

$$T_р = T_0 + \kappa I,$$

где T_0 – постоянная времени анализатора человека, с; I – количество поступающей информации на вход анализатора, бит; κ – семантический коэффициент, характеризующий значимость поступающей информации, с/бит.

С точки зрения информационной характеристики человек является неустойчивой системой. Информационная устойчивость человека была проанализирована в работе [8]. На рисунке 2 представлена область информационной устойчивости по закону Хика [по 8].

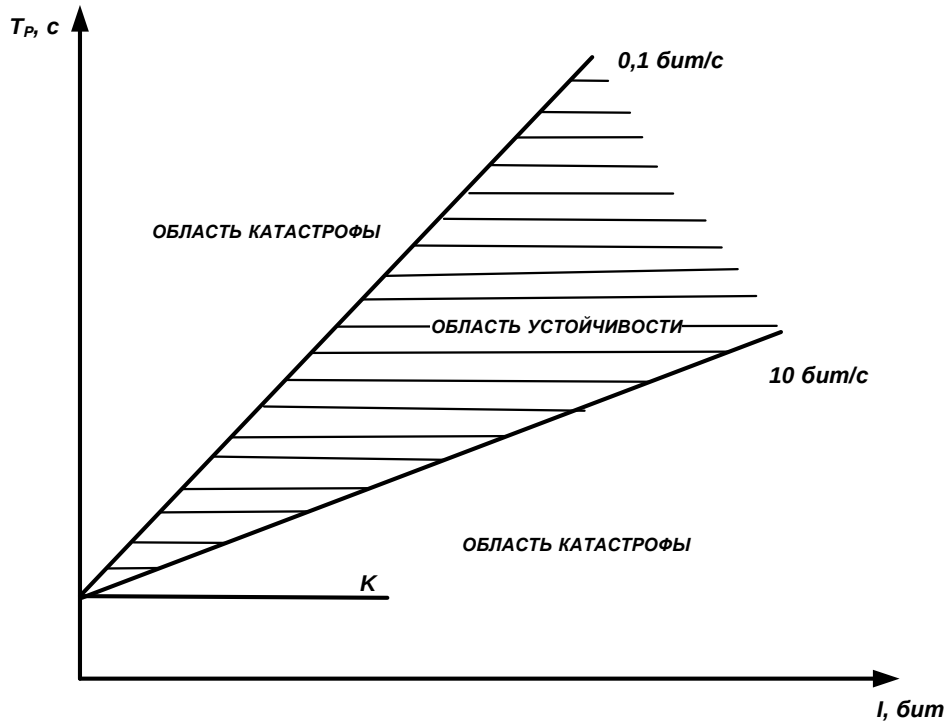

Рисунок 2 – Область информационной устойчивости по закону Хика

Авторы [8] делают вывод о том, что скорость обработки информации человеком можно найти по формуле $V = \int_{f_{min}}^{f_{max}} L\,df$. Подставив в $L = kf^2$

(первый сектор катастроф), получают второй сектор катастроф в виде $V = a f^3 + C$, где a – коэффициент пропорциональности; C – постоянная интегрирования.

Приравнивая правые части равенств, получают третий сектор катастроф (бифуркационное множество):

$$mV^3 + nL^2 = 0,$$

где m и n – коэффициенты пропорциональности.

Объединив эти три сектора, получают уравнение катастрофы–«сборки», характеризующее процесс обработки информации человеком:

$$\frac{1}{4} f^4 + \frac{1}{2} L f^2 + V f = 0.$$

Это уравнение указывает на катастрофическую неустойчивость информационных процессов человека.

Основными характеристиками оператора являются *быстродействие*, *точность*, *надежность*. Оценкой быстродействия оператора является время решения задачи, т.е. время от момента появления сигнала до момента окончания управляющих воздействий.

Вместе с показателями быстродействия технических элементов системы «человек-машина» этот показатель определяет быстродействие всей системы. Оценкой его является время прохождения информации по «человеко-машинному» замкнутому кругу:

$$T_{\text{ц}} = \tau_{\text{оп}} + \sum_{i=1}^{n} Tm_i,$$

где $\tau_{\text{оп}}$ – время обработки информации (решение задачи управления) оператором; n – число звеньев машины; Tm_i – время задержки информации в i-м звене машины.

При заданном времени цикла регулирования $T_{\text{ц}}$ (исходя из общих технических требований к системе) и известных значениях Tm_i требуемое быстродействие оператора должно удовлетворять условию

$$\tau_{оп} \le T_{ц} - \sum_{i=1}^{n} Tm_i = t_{л},$$

где $t_{л}$ – лимит времени, отводимый оператору для решения задачи.

Надежность человека-оператора характеризует его способность выполнять в полном объеме возложенные на него функции при определенных

условиях; она сама характеризуется безошибочностью, готовностью, восстанавливаемостью и своевременностью. Основным показателем безошибочности является вероятность безошибочной работы на уровне отдельной операции и на уровне полного алгоритма в целом.

Коэффициент готовности характеризует вероятность включения человека-оператора в работу в любой произвольный момент времени:

$$k_{оп} = 1 - \frac{T_0}{T},$$

где T_0 – время, в течение которого человек не может принять поступившую к нему информацию; T – общее время работы человека-оператора.

Показатель восстанавливаемости определяется как вероятность исправления оператором допущенной ошибки:

$$P_{исп} = P_к \cdot P_{обн} \cdot P_и,$$

где $P_к$ – вероятность выдачи сигнала схемой контроля; $P_{обн}$ – вероятность обнаружения сигнала оператором; $P_и$ – вероятность исправления ошибочных действий при повторном выполнении алгоритма.

Показатель своевременности характеризует вероятность выполнения задачи в течение времени $\tau \le t_л$, где $t_л$ – лимит времени, превышение которого рассматривается как ошибка. Эта вероятность

$$P_{оп} = P(\tau \le t_л) = \int_0^{t_л} f(\tau) d\tau,$$

где $f(\tau)$ – функция распределения времени решения задачи человеком-оператором.

Показатели надежности системы «человек-машина» определяются через показатели надежности ее звеньев при определенных условиях. Для систем непрерывного типа показателем надежности является вероятность безотказного и безошибочного протекания производственного процесса в течение времени. Такое возможно, если технические средства работают исправно; при их отказе оператор безошибочно и своевременно выполнил требуемые действия или, допустив ошибки в своих действиях, своевременно их исправил. Показатель надежности системы «человек-машина» рассчитывается по формуле:

$$P_{ч.м}(t) = P_т(t) + [1 - P_т(t)]\, K_{оп}\, [P_{оп}\, P_{св} + (1 - P_{оп})\, P_{исп}(T_л)],$$

где $P_т(t)$ – вероятность безотказной работы технических средств.

Надежность человека-оператора – психологическая характеристика человека, обеспечивающая работоспособность регулируемой им системы «человек-машина» в диапазоне различных условий ее существования.

Анализ отечественных и зарубежных исследований свидетельствует о том, что учет психологических показателей является признанным способом обеспечения эффективности и надежности деятельности операторов. Анализ психологических причин чрезвычайных ситуаций, показывает, что большинство ошибок в деятельности оператора обусловлено: интеллектуальным срывом, когда под влиянием стресса нарушается деятельность интеллектуальных функций, связанных с оценкой ситуаций и выработкой решения; неосторожностью (отсутствием страха перед опасностью, возможно вследствие привыкания к ней); беспечностью, недооценкой обоснованности нормативных требований.

Таким образом, учет выше изложенных специфических психофизиологических характеристик человека-оператора, их взаимосвязей и синергии накладывает особенные трудности в обеспечении ИПБ оператора и АС, обусловливает необходимость разработки моделей и методов комплексной экспресс-оценки ПФС как оценки информационной защищенности, а ее решение требует новых подходов.

Проблема оценки информационной защищенности оператора АС в условиях информационных воздействий является производной общей проблемы оценки функционирования автоматизированной системы.

С одной стороны, информационная модель человека позволяет определить сущностные характеристики человека-оператора как объекта обеспечения информационной безопасности. С другой – особенности методов и моделей оценки психофизиологического состояния оператора.

Список литературы

1. Ганеев А.Б. Особенности действия модулированного электромагнитного излучения крайневысоких частот на клетки животных: Автореф.дисс. канд. физ.-мат. наук. – Пущино: ин-т теор. и эксперимент. биофизики РАН, 1997. – 21 с.
2. Гатчин Ю.А., Величко Е.Н., Сухостат В.В. Методология информационно-психологической безопасности личности // Труды Конгресса по интеллектуальным системам и информационным технологиям "IS&IT" Научное издание в 4-х томах. – Москва: Физматлит, 2011. – Т. 2. – С. 338-344.
3. Гатчин Ю.А., Стельмашонок Е.В., Сухостат В.В. Роль деструктивных воздействий внешней среды на безопасность молодежных групп // Методы и технические средства обеспечения безопасности информации: Материалы 28-й научно-технической конференции 24 – 27 июня 2019 года. – СПб.: Изд-во Политехн. ун-та, 2019. – С. 50-52.
4. Гатчин Ю.А., Чиков К.Н. Линия жизни – информационная безопасность / Серия «Выдающиеся ученые Национального исследовательского университета ИТМО», выпуск 17. – СПб.: НИУ ИТМО, 2012. – 270 с.

5. Дружилов С.А. Психология профессионализма. Инженерно-психологический подход. – М. Гуманитарный центр, 2017. – 360 с.
6. Зацаринный А.А., Кисилев Э.В., Козлов С.В., Колин К.К. Информационное пространство цифровой экономики России. Концептуальные основы и проблемы формирования. / Под общей редакцией А.А. Зацаринного. – М.: ФИЦ ИУ РАН, 2018; ООО «НИПКЦ Восход А», 2018 – 236 с.
7. Информационная безопасность цифрового пространства / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб.: Изд-во СПбГЭУ, 2019. – 155 с.
8. Пученков Л.Н. Нестационарные алгоритмы реализации приближенных методов решения дифференциальных уравнений для описания действий оператора ПЭВМ в человеко-машинных системах. – М., 2006. – [Электронный ресурс]. URL: http://lib.znate.ru/docs/index-51215.html (дата обращения: 10.11.2019).
9. Рубин А.Б. Биофизика [Электронный ресурс]. URL: http://www.library.biophys.msu.ru/rubin (дата обращения: 10.11.2019).
10. Сухостат В.В., Тушканов Е.В. Метод оценки работоспособности IT-специалиста в условиях информационного воздействия // Сборник тезисов докладов конгресса молодых ученых, Выпуск 1. – Санкт-Петербург: НИУ ИТМО, 2014. – С. 233.
11. Тулова С.А. Модель обучаемого как средство управления сеансом работы пользователя компьютерной обучающей системы: автореф. дис. на соискание ученой степени к.т.н. – Тверь, 2006. – 16 с.
12. Фугелова Т.А. Инженерная психология. – М.: Юрайт, 2019. – 316 с.

УДК 004.021

Алгоритм выбора рациональной функциональной структуры многостадийных процессов

М. С. Якубов, профессор,
кафедра информационных технологий ТУИТ, Узбекистан
Л. С. Кулдашев, докторант,
НавГПИ, Узбекистан

Разработка алгоритма выбора предпочтительной функциональной структуры процесса для синтеза системы гибкого управления, разработка, поиск и выбор на ранних стадиях проектирования наиболее эффективного варианта многостадийных процессов (МСП) – сложнейшая научно-техническая задача, в которой пересекаются многочисленные организационно-технические и планово-экономические решения. Окончательный выбор этих решений на проектной стадии сопряжен с выявлением наиболее экономичной формы связи между планом производства и производственной структурой, поскольку состав и характеристики последней определяют конечные цели, как отдельных инженерных задач, так и проектируемой системы в целом [1,2].

Формирование организационно-функциональной структуры системы гибкого управления заключается в определении рациональной иерархической структуры управления, которая при прочих равных условиях обеспечивает максимальную отдачу от используемых ресурсов и процессе достижения организацией определение целей.

Производственная структура МСП (рисунок 1) содержит большое разнообразие возможных путей достижения системой поставленных перед ней программой целей при определенных критериях или показателях ее функционирования. Ими могут быт, например, обеспечение наивысшей производительности, наименьшей себестоимости или связанных с ними значений таких величин, как производственная мощность системы и капитальные затраты на ее создание и внедрение.

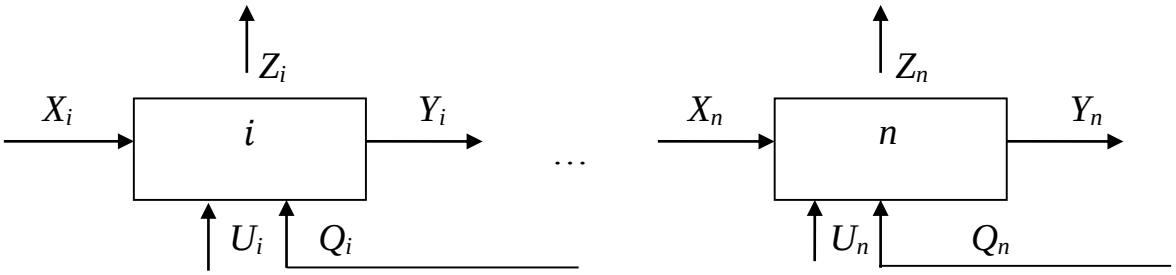

Рисунок 1 – Структурная схема МСП

Здесь $i=1,n$ – число стадий; X_i, Y_i, Z_i, U_i, Q_i – соответственно входные, выходные параметры, помехи, управляющие параметры, циркулирующие параметры.

Существенной чертой создания МСП во многом обуславливающей подход к его организации, является определение состава как технологического, так и информационно-управляющего оборудования путем выбора соответствующих его единиц из числа заданных элементов, имеющихся в распоряжении проектировщика.

С целью оптимизации выбора технологического и информационно-управляющего оборудование и на их основе оптимальной структуры МСП следует перебрать несколько возможных вариантов того или другого оборудования, технологических схем переработки материального ресурса, чтобы выбрать наилучший.

В связи с многовариантным характером технологического проектирования по сравнению с традиционным, одной из задач разработки идеологии системного проектирования и внедрения является определение структуры процесса проектирования, т.е. его последовательности, поскольку именно структуру следует считать доминирующим фактором

успеха, так как решение самих задач оптимизации по этапам есть лишь тактика, а не стратегия.

Задачу выбора технологического оборудования можно разбить на две подзадачи: выбор количественного состава и типов оборудования. В первом случае необходимо при конкретном заданном наборе оборудования выбрать оптимальный и количественный состав оборудования в каждой группе технологического оборудования, занятий в заданном технологическом процессе. Во втором случае необходимо для каждой операции рассматриваемого технологического процесса выбрать из заданного набора оборудование, способные выполнить данную операцию оптимальным образом по некоторым выбранным критериям для данного технологического процесса. На рисунке 2 представлен алгоритм выбора предпочтительной структуры МСП.

Согласно этому подходу основные этапы работы по выявлению рациональной иерархии состоят в следующем:

– априорно формируются некоторые принципы организации иерархического управления;

– в соответствии с ними строится иерархия математических моделей, наделяемых по возможности полным составом свойств, реальных производственных систем и сводящихся к какому-либо известному типу задач математического программирования;

– разрабатываются (или применяются) те или иные разновидности методов декомпозиции задач математического программирования, обеспечивающие согласование решений в данной иерархии математических моделей;

– основные этапы принятого алгоритма согласования получают содержательную интерпретацию в терминах рассматриваемой производственной системы, и рекомендуется как механизм согласования управляющих решений в рамках соответствующей иерархии;

– исходя из качественных соображений намечается несколько возможных вариантов иерархии производственных систем;

– функционирование каждого из них имитируется с помощью принятых методов декомпозиции, и результаты оцениваются по некоторым критериям сравнения вариантов иерархии.

Предполагается, что в итоге удается определить рациональный вариант иерархии управления, рассматриваемой производственной системой. Разнообразие технологических схем и маршрутов переработки сырья обуславливается также широкономенклатурностью исходного сырья, подвергающегося переработке. Построение рациональной структуры и функционирования МСП во многом зависит от объективных факторов, характери-

зующих конкретное производство, таких как объем выпускаемой продукции, производительность, надежность работы, занимаемая Производственная площадь и т.д. Пространственная расстановка оборудования является функцией проектирования производственной системы, и затраты функционирования системы в значительной степени зависят от схемы расположения оборудования. Относительное постоянство расположения оборудования предполагает, что особое внимание следует уделить разработке рациональной схемы его расстановки.

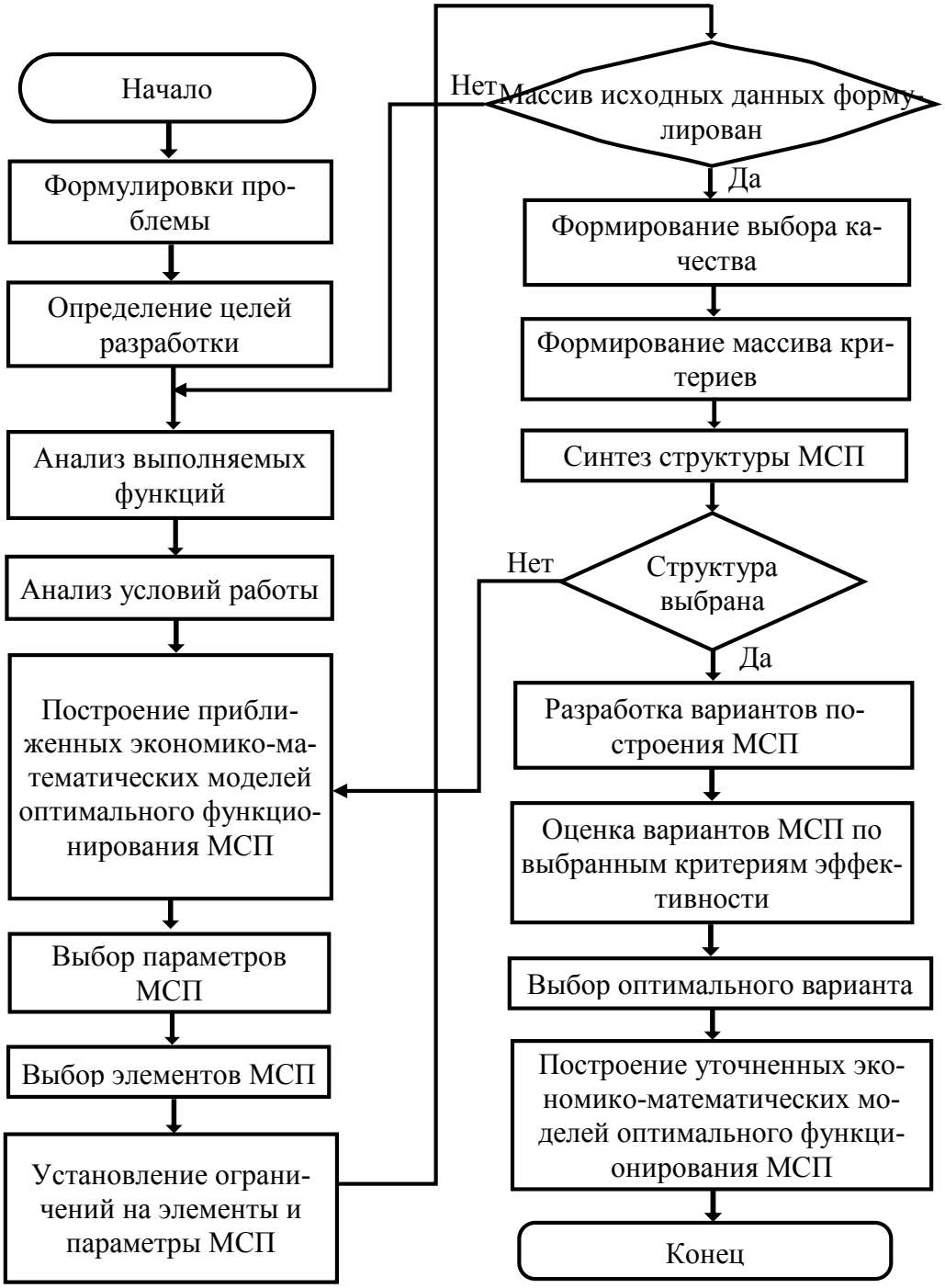

Рисунок 2 – Алгоритм выбора предпочтительной структуры МСП

При создании системы управления МСП необходимо определить структуру МСП, то есть упорядоченное множество технологических переходов $\varphi_j = (\varphi_j^4, \varphi_j^2, \dots, \varphi_j^{\text{к}},)$, воздействие которых на множество $\{a_i\}$ приведет к образованию продукции $\mathcal{A}$

$$\varphi_j = \{a_i\} \to \text{А}, \ \forall \varphi_j \in \Phi$$

При соблюдении технических и технико-экономических требований. Здесь Ф – множество технологических схем, удовлетворяющих необходимо-му условию осуществляемости переработки сырья и выпуска продукции.

Обычно выбор предпочтительной производственно-технологической структуры МСП включает определение такого набора технологических схем производственного процесса и комплекса оборудования для их реализации, которые обращали бы в экстремум целевой функцию Зп или Эп, а также время длительности процесса переработки. Здесь Зп – желаемый эффект при минимуме затрат на переработку сырья в объеме годовой программы выпуска, Эп – максимальный эффект при использовании заданных ограничениях ресурсов.

Принципиальные трудности принятия решения могут быть вызваны на практике наличием множества показателей, с различных сторон, оценивающих техническое устройство. Ни один из этих показателей не обладает функциональные полнотой, поэтому выбор оптимальных решений связан с необходимостью учета множество критериев и решение задачи многокритериальной оптимизации.

Большинство известных методов решения многокритериальных задач ориентировано на решение задач с качественными критериями.

Если выбрать в качестве главного показателя эффективности производственного процесса время длительности процесса переработки материального ресурса, то задача оптимизации может быть сформулирована следующим образом:

$$\mathcal{F}(\varphi_j) = \sum_{i=1}^{n} f(\varphi_j^i) \to min$$

При ограничениях по производительности $n_{min} \le n \le n_{max}$, стоимости оборудования $c_{min} \le c \le c_{max}$, занимаемой площади $n_{\lambda min} \le n_\lambda \le n_{\lambda max}$, надежности работы $\text{Н}_{min} \le \text{Н} \le \text{Н}_{max}$, где $\mathcal{F}(\varphi_j)$ – функция, определяющая время переработки материального ресурса, $f(\varphi_j)$ – функция,

определяющая время на каждой технологические операции, i – число технологических переходов, j – номер технологических схем.

Обобщенная задача синтеза оптимального варианта МСП произвольного вида формируется как определение технологической структуры и аппаратурного состава, при которых обеспечивается заданная производительность по выпуску продукции и номенклатуре и выполняются все технологические и организационные условия и при этом достигается экстремальные значение критерия оптимальности, то есть

$$extr\ R\ (\bar{s}, \bar{\kappa}, \bar{r})$$

при $\mathcal{M}\ (\bar{s}, \bar{\kappa}, \bar{r}) \gtreqless 0$, где $\bar{s}$ – вектор, характеризующий технологическую структуру системы, то есть технологические маршруты производства продуктов и способы коммутации аппаратурных стадий; $\bar{\kappa}$ - вектор, элементами которого являются вещества и определяющие размеры технологических аппаратов, а также их конструкционные параметры; $\bar{r}$ –вектор режимных параметров процесса, учитывающий в обязательном порядке способы функционирования технологического оборудования.

Научно-технический прогресс дает основание предполагать, что расположение оборудования, технологических агрегатов можно будет относительно легко изменять в соответствии с изменяющимся потребностями производства. По всей вероятности, приближение этого времени будет зависеть от успехов в проектирование производственного оборудования, состоящего из независимых унифицированных узлов (агрегатов), которые могут быть перегруппированы в различных пространственных комбинациях в соответствии с экономическими критериями перенастройки. Очевидно, на расположение оборудования внутри предприятия влияет ограниченность числа пространственных комбинаций расстановки оборудования технологических агрегатов, размеры и форма производственной площади. Предварительным решением задачи о расстановке оборудования является определение формы специализации участка, цеха, и производства в целом. В случае принятия решения об организации производственного процесса, отвечающего технологической форме специализации, или если на поточной линии перерабатывается материальный ресурс с разветвленными технологическими маршрутами (схемой), то возникает задача назначение групп оборудования или отдельных агрегатов на различные имеющиеся в наличии места в каком-то ограниченном пространстве. Выбор назначения на различные места часто основывается на таких технико-экономических критериях, как:

– объем, масса или стоимость материального ресурса, протекающего между различными технологическими агрегатами или участками;

– возможное расширение производства и адаптация к изменениям;

– соблюдение требований техники безопасности и охраны труда;

– удобства обслуживания хозяйством производственного назначения;

– снижение загрязнения окружающей среды.

Эффективное использование потенциальных возможностей гибко перенастраиваемой технологии обеспечивается за счет автоматизации информационно-управляющих процессов с применением достаточно универсальных и гибких процедур решения на средствах вычислительной техники задач планирования и управления МСП.

Гибкость производственных процессов и технологий выражается в его перенастраиваемости и характеризуется:

– широтой ассортимента производимой предприятием продукции;

– временем перенастройки перерабатывающей системе на переработку другого вида материального ресурса;

– временем подготовки производства на выполнение новых производственных заданий, т.е. мобильностью производства;

– способностью системы продолжать функционировать при отказе одного или нескольких ее элементов.

При этом свойство гибкости многостадийной производственной системы означает способность ее достаточно быстро перестраивать свою структуру на выполнение нового производственного задания из некоторого класса с учетом характера исходного материального ресурса. Обозначим через $\mathcal{K} = \{\mathcal{Z}_i, i = \overline{r.I}\}$ – класс производственных заданий, которые может эффективно выполнять МСП. Отдельное производственные задания $\mathcal{Z}$ класса $\mathcal{K}$ характеризуется качеством и количеством выпускаемой продукции, свойством исходного материального ресурса – $\mathcal{T}_j$, множеством возможных технологических схем $\mathcal{M}_{j\ell}$ переработки материального ресурса свойством $\mathcal{T}_j$, количество (объемом) перерабатываемого материального ресурса указанного свойства, которое требуются перерабатывать за определенный плановый период:

$$\mathcal{Z}_i = \left\{\left(\mathcal{T}_j, \left\{\mathcal{M}_{j\ell}, \ell \in I, \overline{\mathcal{Z}_j}\right\}, \mathcal{N}_{ij}\right); j = \overline{1, \mathcal{Z}_i}\right\} \quad (1)$$

Для оценки эффективности выполнения производственного задания $\mathcal{Z}_i$ данной МСП ведем коэффициент

$$\eta_i = \frac{\mathrm{T}_i}{\mathrm{T}_i + \Delta_i}, \quad (2)$$

где

$$\mathrm{T}_i = min \sum_{j=1}^{\mathcal{Z}_i} \sum_{l=1}^{\mathcal{Z}_i} \mathcal{T}_{wje} \mathcal{N}_{ijl} \,, \tag{3}$$

$$\Delta_i = \; min \sum_{j=1}^{\mathcal{Z}_i} \sum_{l=1}^{\mathcal{Z}_i} \mathcal{T}_{njl} \,. \tag{4}$$

Минимизация в формуле (3) осуществляется по всевозможным вариантам разбиения $\mathcal{N}_{ij}$ по технологическим схемам с соблюдением условия

$$\sum_{l=1}^{\mathcal{Z}_i} \mathcal{N}_{ije} = \; \mathcal{N}_{ij}, \tag{5}$$

а минимизации в формуле (4) производится по всевозможным вариантам упорядочивания свойств $\mathcal{T}_j$ в задании $\mathcal{Z}_i$; $\mathcal{T}_{wjl}$ время переработки материального ресурса свойством $\mathcal{T}_j$ по ℓ-ой технологической схеме, $\mathcal{T}_{njl}$ –организационные простои основного технологического оборудования (агрегата) при переработке материального ресурса свойством $\mathcal{T}_j$ по ℓ-ой технологической схеме. Обозначим через $\Delta i_1 i_2$ – длительность организационных простоев основного оборудования при переходе с задания $\mathcal{Z}_{i1}$ на задание $\mathcal{Z}_{i2}$. Тогда коэффициент эффективности упорядоченной пары заданий ($\mathcal{Z}_{i1}$, $\mathcal{Z}_{i2}$):

$$\eta_{i_1 i_2} = \frac{\mathrm{T}_{i_1} + \mathrm{T}_{i_2}}{\mathrm{T}_{i_1} + \mathrm{T}_{i_2} + \Delta_{i_1} + \Delta_2 + \Delta_{i_1 i_2}} \tag{6}$$

Эффективность МСП в классе $\mathcal{K}$ описывается матрицей

$$\mathcal{H} = \; \left\| \eta_{i_1 i_2} \right\|_{I \times I}, \tag{7}$$

диагональные элементы которые совпадают с η_i.

Матрица $\mathcal{H}$ может служить для оценки гибкости производственной системы в классе $\mathcal{K}$, выбор рациональных вариантов производственных заданий и порядка следования их друг за другом. Гибкость системы обеспечивается путем наделения системы совокупностью следующих свойств:

– наличие резерва производственных мощностей, что способствует увеличению количества реализуемых вариантов разбиения $\mathcal{N}_{ij}$ согласно (5);

– расширение технологических возможностей основного оборудования, что способствует расширению класса $\mathcal{K}$ и увеличению числа возможных маршрутов $\mathcal{Z}_i$ в конкретном производственном задании (1), что одновременно уменьшает $\mathcal{Z}_i$ и Δ_i в (3) и (4);

– возможность выбора различных технологических схем переработки сырья, что позволяет увеличить $\mathcal{Z}_i$ и уменьшить Δ_i в формуле (2);

– возможность оперативного изменения производственных расписаний, что позволяет уменьшить в выражении (4) и тем самым, уменьшить Δ_i;

– расширение класса возможных производственных заданий.

Следует также отметить, что для выбора оптимального варианта производственной структуры предприятия, состоящий из набора структурных единиц различных типов, необходимо четкая классификация последних. На промышленном предприятии структурные единицы различаются по основным признакам: методу производства, ассортименту перерабатываемого материального ресурса, непрерывности технологических процессов, степени автоматизации технологических процессов, а самые же условия производства – по несколько иным признакам: по структурно-технологическому сходству технологических процессов переработки, виду требуемого оборудования и масштабу выпуска продукции.

Предварительная классификация структурных единиц по указанным признаком позволяет ограничить перебор их возможных вариантов с целью выбора варианта, который наибольшей степени соответствует условиям данного производства.

Процесс синтеза структуры система гибкого управления МСП в общем случае, когда определен оптимальный вариант размещения множество технологических процессов на оборудование действующие схемы, заключается в организации такой стратегии, при которой обеспечивается минимум суммарных потерь от простоев технологического оборудования.

$$\sum_{a\in\mathcal{A}}\sum_{s\in\mathcal{S}}\int_{\mathcal{T}_0}^{\mathcal{T}}\mathcal{F}(\mathcal{T})d\mathcal{T}\rightarrow min,$$

где $\mathcal{F}(\mathcal{T})$ – функция потерь от простоя аппарата $a\in\mathcal{A}$ в состоянии ожидания $s\in\mathcal{S}$.

Системная модель организации процессов и аппаратов имеет вид:

$$\mathcal{M}_{0\rho}=<\mu,\mathcal{v},w>,$$

где $\mu,\mathcal{v},w$ – соответственно множество моделей организации процессов в аппаратах периодического действия и моделей их взаимодействия, аксиоматические модели произвольных взаимодействий аппаратов или аппаратурных стадий.

В переделах каждой технологической операции СУ осуществляет функции информационного контроля и регулирования технологических параметров и выполняет оптимальный переход от одной операции к другой,

реализует требуемый в данный момент закон регулирования, подключает регулирующие устройства к регулирующим органом, изменяет величину задание регулятором.

Список литературы

1. Yakubov M.S., Kubaev U.R., Varisov A.A., Turgunov M.R. Logistics Features of the information resources in the electronic document circulation. Science and world. International scientific journal, №3 (19), 2015, Vol.I I, ISSN 2308-4804. – P.107-111.
2. Якубов М.С., Кубаев У.Р. Многостадийные процессы формирования электронного правительство //SCIENCEAND WORLD International scientific journal №3 (31), 2016,Vol.I ISSN2308-4804 – С. 104-107.
3. Якубов М.С., Кубаев У.Р., Варисов А.А., Тургунов М.Р. Особенности логистики информационных ресурсов в электронном документообороте // SCIENCE AND WORLD International scientific journal №3 (19),2015,Vol.II ISSN2308-4804 – С. 107-111.
4. Гафуров Ю., Якубов М. Автоматизация процессов производства стекольной промышленности и уменьшение финансовых потерь // Модернизация системы местного управления: зарубежный опыт и реформы в Узбекистане. Сборник материалов международной научно-практической конференции. Ташкент, 2017 год 14 июня. – Ташкент, 2017. – С. 301-305.
5. Якубов М.С., Тургунов М.Р. Создание интегрированной системы управления грузопотоками железнодорожного транспорта // Вестник ТашГТУ, 86-90 с. №1. – Ташкент, 2017.

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

Сборник научных статей

Под редакцией Е.В. Стельмашонок, И.Н. Васильевой

Подписано в печать 27.12.19. Формат 60×84 1/16.
Усл. печ. л. 10,25. Тираж 500 экз. Заказ 1967.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ