вий и безопасности на предприятии, что может привлечь квалифицированных специалистов и повысить уровень производительности. Энергетическая эффективность помогает предприятиям сократить свои операционные расходы и улучшить свою финансовую устойчивость.

Список литературы

1. Соломин С.А., Преображенский Ю.П. Проблемы обеспечения функционирования энергетических систем // Проблемы развития современного общества: сборник научных статей 7-й Всероссийской национальной научно-практической конференции. В 5-ти томах. Том 4. 2022. С. 345-348.

2. Львович И.Я. О возможностях автоматизации при повышении эффективности энергетических систем // Современные материалы, техника и технология. 2020. С. 220-223.

3. Львович И.Я. Проблемы автоматизации управления энергетическими системами // Современные материалы, техника и технология. 2020. С. 216-219.

4. Сафаров И.М., Давлетхузина Э.М., Ишмухаметова Д.М., Баширова Л.И., Садыков Р.Д., Хлебников Д.А. Состояние уровня автоматизации энергетических объектов и решения, направленные на его повышение // Инженерный вестник Дона. 2021. №1 (85). URL: ivdon.ru/ru/magazine/archive/n1y2021/7382 (дата обращения: 07.09.2023).

5. Клаусснер В.А., Демкин В.И. Анализ применения автоматизированной системы коммерческого учета электроэнергии в промышленности // Молодой ученый. 2021. № 5 (347). С. 33-35.

СТОИМОСТНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кислова Д.А., Аветисян Т.В.

Колледж Воронежского института высоких технологий, Воронеж, e-mail: vtatyana_avetisyan@mail.ru

Информационная безопасность включает в себя различные меры по защите информации от несанкционированного доступа. В прошлом, в эпоху до цифровых технологий, люди использовали сейфы для хранения важных документов, нанимали охранников и шифровали свои сообщения на бумаге. В настоящее время защита информации чаще всего относится к цифровой сфере, но основные принципы остаются прежними: специалисты по информационной безопасности создают защищенные виртуальные пространства, устанавливают защитное программное обеспечение, например, антивирусы и используют криптографические методы для шифрования цифровой информации [1].

Информационная безопасность включает в себя защиту трех основных аспектов информации: ее конфиденциальности, целостности и доступности. В рамках концепции информационной безопасности эти аспекты называются принципами информационной безопасности.

Конфиденциальность гарантирует, что информация доступна только тем, кому она предназначена, и не попадает в руки посторонних лиц. Целостность обеспечивает сохранность и неприкосновенность информации, чтобы она не была изменена или повреждена без разрешения. Доступность означает, что информация доступна и используется в нужное время и месте Эти принципы информационной безопасности являются основой для разработки соответствующих мер и политик, направленных на защиту информации от угроз и несанкционированного доступа.

Надежная система защиты должна соответствовать следующим принципам [2,3]:

1) Затраты на внедрение и поддержку системы защиты не должны превышать потенциальные потери от возможных нарушений безопасности;

2) Каждый пользователь обязан иметь доступ только к тем функциям и данным, которые необходимы для выполнения его задач, чтобы минимизировать риски несанкционированного доступа и злоупотребления;

3) Системе защиты необходимо быть удобной и интуитивно понятной для пользователей, чтобы они могли эффективно выполнять свои задачи без излишних препятствий;

4) Система защиты должна иметь механизмы для быстрого отключения или обхода в случае чрезвычайных ситуаций, например, при возникновении угрозы жизни или критических сбоев.

5) Система защиты обязана обеспечивать безопасность всех компонентов и данных, используемых в процессе обработки информации, включая серверы, сети, базы данных и приложения;

6) Разработчики системы защиты не должны иметь привилегированный доступ или контроль над системой, чтобы предотвратить возможность злоупотребления и конфликта интересов.

Стоимостная составляющая надежной системы защиты имеет несколько аспектов [4,5]:

Первый аспект стоимостной составляющей информационной безопасности – это затраты на оборудование и программное обеспечение. Установка и поддержка физической и логической инфраструктуры, таких как серверы, межсетевые экраны, антивирусные программы и системы защиты данных, требует значительных расходов. Компании, особенно крупные организации, должны иметь надежные аппаратные и программные средства для обеспечения безопасности своих информационных ресурсов.

Второй аспект связан с затратами на персонал. Специалисты по информационной безопасности являются ключевыми фигурами в обеспечении безопасности систем и сетей. Это профессионалы, которые не только создают и настраивают системы защиты, но и мониторят их работу, анализируют уязвимости и реагируют на возможные инциденты безопасности. Работа таких высококвалифицированных специалистов требует значительных финансовых ресурсов для их найма и обучения, а также для удержания в компании.

Третий аспект – затраты на обучение и осведомленность сотрудников. Помимо IT-специалистов, все сотрудники организации должны быть осведомлены о принципах и практиках информационной безопасности. Бездействие или неосторожное отношение к безопасности может привести к серьезным угрозам, включая утрату данных, взлом системы или нарушение конфиденциальности. Обучение сотрудников включает проведение семинаров, разработку политик и процедур, а также постоянное напоминание о безопасности информации. Эти затраты на обучение и повышение осведомленности персонала также включаются в общую стоимость информационной безопасности.

Четвертый аспект стоимости информационной безопасности связан с рисками и потенциальными угрозами. Информационные атаки, вирусы и другие угрозы могут причинить серьезный ущерб компании. Поддержание высокого уровня защиты может предотвратить такие атаки и снизить риски финансовых потерь. Ведение пассивной политики безопасности и недостаточные меры защиты могут привести к серьезным последствиям, таким как потеря репутации, судебные иски и прочие потери, как для компании, так и для ее клиентов.

Формула стоимостных аспектов информационной безопасности может включать в себя следующие составляющие:

1. Затраты на приобретение и внедрение средств защиты информации, такие как аппаратное и программное обеспечение, обучение персонала и т.д.

2. Затраты на поддержание и обновление систем информационной безопасности, включая расходы на обслуживание, лицензионные платежи, анализ уязвимостей и т.д.

3. Потери от возможных инцидентов информационной безопасности, такие как утечки данных, кражи конфиденциальной информации, вредоносные программы и др. Оценка таких потерь может включать в себя не только прямые финансовые убытки, но и репутационный ущерб, потерю клиентов и бизнеса, судебные издержки и т.д.

4. Экономический эффект от защиты информации, включая уменьшение рисков и потерь, повышение доверия клиентов и партнеров, усиление конкурентных преимуществ и т.д.

Список литературы

1. Преображенский Ю.П. Информационная безопасность – вызовы современного мира // Вестник Воронежского института высоких технологий. 2017. № 2(21). С. 60-63.

2. Смыкова В.Н., Нечволода В.Э., Орел Д.В. Экономические аспекты информационной безопасности // Студенческая наука для развития информационного общества: сборник материалов X Всероссийской научно-технической конференции с международным участием, Ставрополь, 07–08 ноября 2019 года. Том Часть 1. Ставрополь: Северо-Кавказский федеральный университет, 2019. С. 162-169.

3. Балашова А.В., Преображенский Ю.П. Проблемы обеспечения безопасности в информационных системах // Молодежь и XXI век. 2022. С. 15-19.

4. Компанейцева Г.А. и др. Стоимостные аспекты в концепции экономической безопасности компании // Вестник Московского финансово-юридического университета. 2017. № 3. С. 95-103.

5. Мандрица И.В., Мандрица О.В., Соловьева И.В., Петренко В.И. Метод обоснования затрат на информационную безопасность бюджетных организаций // Вестник Северо-Кавказского федерального университета. 2017. № 1(58). С. 67-71.

КОМПЬЮТЕРНАЯ ГРАФИКА НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

Макаров П.В., Наумова А.И.

МОУ "Тверской лицей", Тверь, e-mail: a_naumova_46@mail.ru

В процессе исследования формальных моделей часто производится их *визуализация*. Для визуализации алгоритмов используются *блок-схемы*, пространственных соотношений параметров объектов – *чертежи*, моделей электрических цепей – *электрические схемы*. При визуализации формальных моделей с помощью анимации может *отображаться динамика процесса*, *производится построение графиков изменения величин* и т. д.

В настоящее время широкое распространение получили *компьютерные интерактивные визуальные модели*. В таких моделях исследователь может менять начальные условия и параметры протекания процессов и наблюдать изменения в поведении модели.

Используя *компьютерную визуализацию*, в 2022-2023 году в Тверском лицее под руководством преподавателя информатики высшей категории А.И. Наумовой ученик 10 физико-математического класса Макаров Пётр написал научную работу на тему: "Исследование информационных моделей из курса математики на языке программирования Python ".

Цель данной работы заключается в том, чтобы получить *дополнительные знания* по этой теме и *научиться проводить исследования решений математических задач с помощью построения графиков.*

Работа состоит из двух частей: *описательной* (дана характеристика основных этапов разработки информационных моделей) и *практической* (приведён пример разработки алгоритма и программы (скрипта) *полного исследования квадратного уравнения* с использованием вложенных сложных условий, подключения модулей для работы с графикой и созданием функций пользователя с последующей обработкой данных на компьютере). Показаны примеры выполнения программы (скрипта) как в среде программирования, так и выполнение созданного файла .exe.