высших учебных заведениях усилиями специалистов, профессорско-преподавательского состава, а также студентов подготовлена программа сетевого обеспечения цифрового образования, разработаны соответствующие порталы.

Наша страна является активным сторонником привлечения новаций во все сферы жизнедеятельности, включая область телекоммуникаций и высокоскоростных информационных технологий. Туркменистан открыт для всего нового в мировом опыте, с учётом национальных интересов и задач социально-экономического и духовно-культурного развития строит прочные отношения с государствами планеты, сотрудничает с зарубежными институтами и авторитетными организациями.

Список использованных источников

1. Круглинский И.К., Абдуллина С.В. Управление трудом в различных сферах жизни человека: поиски универсальных детерминант. - Интернет-журнал «НАУКОВЕДЕНИЕ» №1, 2013
2. Плеханов А.Г. Управление персоналом: учеб. пособ. / А.Г.Плеханов. – Самарск. гос. арх. – строит. Ун-т. Самара, 2005.

УДК 681.3:553.98(574.4)

К. Чарыев[1], А. Чарыева[2]

[1]Международный университет нефти и газа имени Ягшыгельди Какаева
[2]Туркменский государственный институт экономики и управления
Ашхабад, Туркменистан

РОЛЬ КИБЕРБЕЗОПАСНОСТИ В ЭКОНОМИЧЕСКОЙ СФЕРЕ

Аннотация. *В статье рассматривается вопрос кибербезопасности, представляющий собой растущий вызов для устойчивого экономического развития. Кибербезопасность – это защита компьютеров, сетей, программных приложений, критически важных систем и данных от потенциальных цифровых угроз. Организации несут ответственность за обеспечение безопасности данных, чтобы сохранять доверие клиентов и соответствовать нормативным требованиям.*

K.Charyyev[1], A.Charyyeva[1]

[1]Yagshigeldi Kakaev International University of Oil and Gas
[2]Turkmen State Institute of Economics and Management
Ashgabat, Turkmenistan

THE ROLE OF CYBER SECURITY IN THE ECONOMIC SPHERE

Abstract. *The article examines the issue of cybersecurity, which represents a growing challenge for sustainable economic development. Cybersecurity is the protection of computers, networks, software applications, critical systems and data from potential digital threats. Organizations have a responsibility to ensure data security to maintain customer trust and comply with regulatory requirements.*

Кибербезопасность представляет собой растущий вызов для устойчивого экономического развития. Инциденты в киберпространстве могут влиять на безопасность, процветание и устойчивость любой страны и способны подрывать выгоды от происходящей в ней цифровой трансформации. Повышение кибербезопасности и потенциала в киберпространстве становится все более приоритетной задачей как для развитых, так и для развивающихся стран [1].

Кибербезопасность – это защита компьютеров, сетей, программных приложений, критически важных систем и данных от потенциальных цифровых угроз. Организации несут ответственность за обеспечение безопасности данных, чтобы сохранять доверие клиентов и соответствовать нормативным требованиям. Они применяют меры по кибербезопасности и используют специальные инструменты для защиты конфиденциальных данных от несанкционированного доступа и предотвращения сбоев, вызванных нежелательной сетевой активностью, при выполнении бизнес-операций. Организации обеспечивают кибербезопасность, оптимизируя методы цифровой защиты для сотрудников, процессов и технологий.

Компании в различных отраслях, таких как энергетика, транспорт, розничная торговля и промышленность, используют цифровые системы и высокоскоростное подключение, чтобы обеспечивать эффективное обслуживание клиентов и экономичные бизнес-операции. Подобно тому, как они защищают свои физические активы, им необходимо также обеспечивать безопасность своих цифровых ресурсов, а также защищать свои системы от непреднамеренного доступа. Преднамеренный взлом компьютерных систем, сетей или подключенных устройств и получение к ним несанкционированного доступа называется кибератакой. Успешно выполненная кибератака может привести к раскрытию, похищению, удалению или изменению конфиденциальных данных.

Безопасность информации, которая обрабатывается в организации, – это комплекс действий, направленных на решение проблемы защиты информационной среды в рамках компании. При

этом информация не должна быть ограничена в использовании и динамичном развитии для уполномоченных лиц [2].

Требования к системе защиты ИБ

Защита информационных ресурсов должна быть:

1. Постоянной. Злоумышленник в любой момент может попытаться обойти модули защиты данных, которые его интересуют.

2. Целевой. Информация должна защищаться в рамках определенной цели, которую ставит организация или собственник данных.

3. Плановой. Все методы защиты должны соответствовать государственным стандартам, законам и подзаконным актам, которые регулируют вопросы защиты конфиденциальных данных.

4. Активной. Мероприятия для поддержки работы и совершенствования системы защиты должны проводиться регулярно.

5. Комплексной. Использование только отдельных модулей защиты или технических средств недопустимо. Необходимо применять все виды защиты в полной мере, иначе разработанная система будет лишена смысла и экономического основания.

6. Универсальной. Средства защиты должны быть выбраны в соответствии с существующими в компании каналами утечки.

7. Надежной. Все приемы защиты должны надежно перекрывать возможные пути к охраняемой информации со стороны злоумышленника, независимо от формы представления данных.

Для защиты данных используются различные инструменты кибербезопасности, такие, как криптографические протоколы, которые позволяют шифровать электронную почту, файлы и другие важные данные. Этот механизм не даёт перехватить данные или получить код доступа к ним. Поэтому создаются и разрабатываются программы, которые проверяют устройства на наличие вредоносного кода, а после с помощью них отслеживают и удаляют спрятанный в основной записи систем вирус.

Защитные средства обнаруживают вредоносные программы в режиме реального времени, многие из них применяют различный анализ — следят за действиями вредоносной программы и ее кода. Это помогает бороться с вирусами и троянцами, которые могут менять свою структуру. Защитные инструменты умеют изолировать потенциальное вредоносное программное обеспечение в специальной виртуальной среде (подальше от сети пользователя), чтобы затем проанализировать его поведение и научиться лучше распознавать новые источники угроз.

На практике создание системы защиты информации осуществляется в три этапа.

На первом этапе разрабатывается базовая модель системы, которая будет функционировать в компании. Для этого необходимо проанализировать все виды данных, которые циркулируют в фирме и которые нужно защитить от посягательств со стороны третьих лиц.

Второй этап включает разработку системы защиты. Это означает реализовать все выбранные способы, средства и направления защиты данных.

Система строится сразу по нескольким направлениям защиты, на нескольких уровнях, которые взаимодействуют друг с другом для обеспечения надежного контроля информации.

Правовой уровень обеспечивает соответствие государственным стандартам в сфере защиты информации и включает авторское право, указы, патенты и должностные инструкции. Грамотно выстроенная система защиты не нарушает права пользователей и нормы обработки данных.

Организационный уровень позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и физическими носителями данных.

Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством компании совместно со службой безопасности и поставщиком, который внедряет систему безопасности. Цель – создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

Технический уровень условно разделяют на физический, аппаратный, программный и математический подуровни.

- ✓ Физический – создание преград вокруг защищаемого объекта: охранные системы, зашумление, укрепление архитектурных конструкций;
- ✓ аппаратный – установка технических средств: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей;
- ✓ программный – установка программной оболочки системы защиты, внедрение правила разграничения доступа и тестирование работы;

- ✓ математический – внедрение криптографических и стенографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.

Третий, завершающий этап – это поддержка работоспособности системы, регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз.

Список использованных источников

1. Чарыева Д.Д., Агаева Д.М. Основы защиты информации и особенности построения кибербезопасности. Всемирный ученый, 2023.
2. Ш. Закиров. Информационная безопасность: конспект лекций, Челябинск: Издательский центр ЮУрГУ, 2014.

УДК 681.3:553.98(574.4)

Д.Д. Чарыева, А. Ходжагелдиев, И.Г. Аширов, М. Чуриев
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗВОНКА И СИСТЕМЫ ОПОВЕЩЕНИЯ В УЧЕБНЫХ ЗАВЕДЕНИЯХ

Аннотация. *В статье рассматривается проблема создания своими силами системы звонка и оповещения в учебных заведениях. Разработанное авторами достаточно простое, но в тоже время функциональное программное обеспечение позволяет редактировать порядок и время звонков, мелодию звонка и длительность его проигрывания, оповещать речевым сопровождением. Программу можно использовать в любом учебном заведении.*

D.J. Charyyeva, A. Hojageldiyev, I.G.Ashirov, M. Churiyev
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

SOFTWARE OF RING AND NOTIFICATION SYSTEMS IN EDUCATIONAL INSTITUTIONS

Abstract. *The article discusses the problem of creating a bell and notification system in educational institutions on your own. The fairly simple but at the same time functional software developed by the authors allows you to edit the order and time of*