УДК 004.056

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Борисик М.Д., Кресло И.А.
Научный руководитель: ст. преподаватель Ковалькова И. А.
Белорусский национальный технический университет

В современном мире Интернет, играет огромную роль. С помощью Интернета можно хранить различного рода информацию, делиться информацией с другими пользователями. Так как Интернет является общей открытой сетью, то существуют люди (злоумышленники), которые хотят получить какие-либо данные незаконным способом. Тем более, что в современном мире уже существуют и используются технологии, которые создают новые возможности для злоумышленников. Для незаконного получения конфиденциальной информации используются различные средства, например, вредоносное программное обеспечение (ПО), фишинг, DOS-атаки и многие другие. Поэтому, чтобы не допустить утечку информации, незаконное получение данных из Интернета люди начали использовать средства защиты от киберугроз.

Кибербезопасность – это защита подключённых к Интернету систем (оборудования, программного обеспечения и данных) от киберугроз. Также это незаменимый компонент современной жизни, который необходим для защиты информации, данных и личной жизни.

Основная цель кибербезопасности – это защита информационных систем, данных и ресурсов от несанкционированного доступа, кражи, создание гарантий, что защищаемые данные будут целы, не удалены и не изменены. Обеспечение кибербезопасности на практике реализуется с использованием защитных механизмов, при создании которых могут быть использованы различные средства. К ним относятся: программные, аппаратные, физические, программно-аппаратные (или технические), организационные, правовые, криптографические, морально-этические. [1]

Физические

Физическое обеспечение информационной безопасности представляется в виде электронной, механической техники, которая предназначена для создания физиологических препятствий на возможных путях вторжения, а также для получения нелегального доступа преступников к каким-либо составляющим систем или данных.

Также к этой категории относятся визуальное наблюдение, сигнализация, связные устройства. Физическая кибербезопасность связана с

осуществлением защитных мер для защиты от чрезвычайных происшествий (ЧП).

Аппаратные

Аппаратное обеспечение кибербезопасности представляет собой обширную категорию, где представлены различные электронные и механические приборы, интегрированные в автоматизированную информационную систему или работающие как автономная аппаратура, связанная с ним.

Основной задачей аппаратных средств является обеспечение внутренней защиты структурных элементов вычислительных систем, таких как центральные процессоры, периферийные устройства, терминалы и другие. Это реализуется с использованием идентификационных технологий, методов испытаний, проверки полномочий участников, протоколов и реакции на безопасность.

Программные

Программное обеспечение информационной безопасности используется для реализации логико-интеллектуальных защитных функций. Оно может быть добавлено в программное обеспечение автоматизированных информационных систем, либо включено в структуру систем контроля.

В настоящее время реализуется много видов операционных систем, пакетов сетевого управления, пакетов приложений, в которые входят различные средства безопасности данных, в том числе и антивирусные средства.

Программное обеспечение является одним из самых востребованных и повсеместно применяемых видов защиты, так как отличается универсальностью, простотой эксплуатации, имеет возможность изменения и развития. В связи с этим оно считается самой уязвимой частью информационной системы.

Аппаратно-программные

Аппаратные и программные средства защиты кибербезопасности представляют собой различные электронные устройства, гаджеты, оборудование, специальное программное обеспечение, входящее в структуру автоматизированной системы организации, и выполняющие самостоятельно или совместно с другими средствами функции защиты аттестационных и идентификационных процедур, процессов ограничения доступа к информации. [2]

Криптографическую защиту информации можно реализовать при помощи аппаратного или программного обеспечения. Криптографические подходы к защите информации опираются на принципы шифрования информации. Защитные средства данных производят криптографические преобразования информации, чтобы обеспечить её защиту и безопасность.

Административные

Основная задача реализации административных мер по обеспечению кибербезопасности является формирование информационной политики конкретной организации и дальнейшее её выполнение, выделив все необходимые ресурсы и полный контроль за её функционированием.

Правовые

Правовые средства защиты кибербезопасности представляют собой действующие государственные законы, указы президента, нормативные документы, требования и технические регламенты органов регуляторной сферы. С помощью подобных официальных документов регламентируются Правила взаимодействия с информацией, закрепляются права и обязательства участников информационной деятельности при обработке и использовании данных, и устанавливается административная и уголовная ответственность за нарушение законодательства.

Морально-этические

Методы морально-этического обеспечения кибербезопасности относятся профилактическим методам, и поэтому руководство организации должно формировать в коллективе здоровый моральный климат для снижения вероятности возникновения нарушений в информационной среде. [3]

Несоблюдение моральных и нравственных норм поведения в конкретной организации приводит к утрате её авторитета и престижа. В свете быстрого развития технологий и увеличения количества угроз кибербезопасности важно помнить о необходимости соблюдения этических принципов и правильного использования данных. Игнорирование этих аспектов, может привести к необоснованным нарушениям конфиденциальности, нарушению прав пользователей и другим нежелательным последствиям.

В связи с постоянным увеличением сложности и масштабности угроз кибербезопасности, необходимым является постоянное развитие и совершенствование методов и технологий для обеспечения безопасности, а также укрепление сотрудничества между государственными органами, компаниями и экспертами в области кибербезопасности.

Литература

1. Кибербезопасность и информационная безопасность. [Электронный ресурс]. Режим доступа https://spravochnic k.ru/informacionnaya_ bezopasnost/ kiberbezopasnost _i_informacionnaya_ bezopasnost, свободный.

2. Технические средства обеспечения безопасности: Учебное методическое пособие Т38 / Под ред. И. Е. Зуйкова. – Мн.: БГПА., 2021.