# КИБЕРБЕЗОПАСНОСТЬ В ОБРАЗОВАНИИ: ЗАЩИТА ДАННЫХ И ИНФОРМАЦИОННЫХ РЕСУРСОВ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Можейко В.Д., Федоренко В.А.

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь, vlad.mozheiko99@mail.ru*

Abstract. Cybersecurity is an important aspect in higher education systems.

Образовательные учреждения сталкиваются с растущими угрозами в области кибербезопасности. Защита данных и информационных ресурсов становится все более важной в свете увеличивающегося количества кибератак, направленных на учебные заведения. Это вызывает необходимость принятия комплексных мер по защите цифровой инфраструктуры и конфиденциальности данных [1].

Причины, по которым образовательные учреждения становятся объектами кибератак, разнообразны. Одной из причин является большой объем ценной информации, хранящейся в системах учебных заведений, включая личные данные студентов, финансовые документы и исследовательские материалы. Кроме того, часто образовательные учреждения имеют слабые меры защиты и уязвимости в своих информационных системах, что делает их легкой мишенью для киберпреступников.

Для обеспечения кибербезопасности в образовательных учреждениях необходимо рассматривать несколько аспектов:

Во-первых, это разработка и внедрение политики безопасности информации, которая включает в себя установку паролей, шифрование данных, регулярное обновление программного обеспечения и обучение персонала основам кибербезопасности [1].

Второй аспект − это использование современных технологий и инструментов для защиты информации. Это включает в себя установку антивирусного и антишпионского программного обеспечения, использование брандмауэров и систем обнаружения вторжений, а также резервное копирование данных для обеспечения их сохранности в случае кибератаки или системного сбоя.

Третий аспект − это сотрудничество и обмен опытом между образовательными учреждениями и специалистами по кибербезопасности. Образовательные учреждения должны активно сотрудничать с индустрией информационной безопасности, чтобы получить поддержку и экспертные знания по защите от киберугроз [2].

Одним из наиболее важных аспектов информационной безопасности в сфере образования является безопасность баз данных высших учебных заведений. В наше время, когда цифровизация проникает во все сферы нашей жизни, защита данных становится приоритетной задачей для любого учебного учреждения.

Базы данных высших учебных заведений содержат огромное количество ценной информации, включая личные данные студентов, финансовую информацию, учебные материалы, научные исследования и многое другое [1]. Эта информация является не только важным активом учебного заведения, но и ценным ресурсом для злоумышленников, которые могут использовать ее в своих целях.

Одной из наиболее серьезных угроз безопасности баз данных является кибератаки. Злоумышленники могут использовать различные методы атак, такие как взлом паролей, инъекции SQL, кража данных и другие, чтобы получить доступ к информации в базах данных. В результате таких атак может произойти утечка конфиденциальной информации, что приведет к серьезным последствиям для учебного заведения и его студентов.

Для обеспечения безопасности баз данных высших учебных заведений необходимо принять ряд мер. Прежде всего, необходимо установить строгие политики безопасности данных и следовать им. Это включает в себя установку сложных паролей, шифрование данных, регулярное обновление программного обеспечения и мониторинг сетевой активности для обнаружения потенциальных угроз.

Кроме того, необходимо обеспечить физическую безопасность серверов и хранилищ данных, где хранится информация.

Только авторизованным лицам должен быть доступ к оборудованию и базам данных, а помещения с серверами должны быть защищены от несанкционированного доступа.

Важным аспектом обеспечения безопасности баз данных является обучение персонала. Все сотрудники, имеющие доступ к данным, должны быть обучены правилам безопасности информации и знать, как правильно обращаться с конфиденциальными данными, чтобы предотвратить утечки или несанкционированный доступ [2].

Кибербезопасность играет ключевую роль в обеспечении целостности, конфиденциальности и доступности данных в образовательных учреждениях. Она требует не только технических решений, но и стратегического подхода и внедрения соответствующих политик и процедур. Только путем совместных усилий и постоянного внимания к кибербезопасности мы сможем обеспечить защиту данных и информационных ресурсов образовательных учреждений.

**Литература**

1. Мельников. Организация и обеспечение безопасности информационно-технологических сетей и систем [2012]

2. Информационная безопасность - защита и нападение. Защита баз данных. 2-е издание [2017] Бирюков