УДК 004.056

Невлад Ю. В.
ст. преп.,
Невлад Ю. Г.
ст. преп.
Донбасский государственный технический университет, г. Алчевск, ЛНР, Россия

КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ

В современном мире кибербезопасность является одной из важнейших задач для всех сфер жизни, включая образование. Школы, колледжи и университеты используют цифровые технологии для обучения, общения и управления. Это делает их уязвимыми для киберугроз, которые в образовании могут быть направлены на учащихся, преподавателей и сотрудников, а также на информационные системы и ресурсы образовательных организаций.

К наиболее распространенным угрозам относятся: взлом — это несанкционированный доступ к компьютерной системе или сети. Хакеры могут использовать этот доступ для кражи данных, распространения вредоносного программного обеспечения (ПО) или нарушения работы систем. Хищение данных — это несанкционированное получение конфиденциальной информации, такой как персональные данные учащихся, преподавателей или сотрудников, эта опасность может привести к утечке информации, мошенничеству или шантажу. Распространение вредоносного ПО — это передача вредоносных программ, таких как вирусы, трояны или шпионские программы, что может нанести ущерб компьютерным системам и данным, а также может быть использовано для получения персональной информации или контроля над компьютером.

Для защиты учащихся и образовательных организаций от киберугроз необходимо принимать следующие меры:

– обучение пользователей кибербезопасности. Учащиеся, преподаватели и сотрудники должны быть осведомлены о киберугрозах и знать, как защитить себя от них;

– использование надежных технологий и программного обеспечения. Образовательные организации должны использовать надежные технологии и программное обеспечение, которое имеет встроенные средства защиты от киберугроз;

– регулярное обновление программного обеспечения. Образовательные организации должны регулярно обновлять программное обеспечение, чтобы устранить уязвимости, которые могут быть использованы злоумышленниками;

– использование брандмауэра. Брандмауэр — это программное обеспечение, которое защищает компьютерную сеть от несанкционированного доступа;

– использование антивирусного программного обеспечения. Антивирусное программное обеспечение защищает компьютеры от вредоносного ПО;

– резервное копирование данных. Резервное копирование данных позволяет восстановить их в случае взлома или другого инцидента.

Кибербезопасность в образовании является важной задачей, которая требует совместных усилий учащихся, преподавателей, сотрудников и образовательных организаций. Принимая необходимые меры, можно защитить учащихся и образовательные организации от сетевых угроз, обеспечить безопасность информационных систем в цифровом мире. Резервное копирование данных — это процесс создания копий важных данных, которые можно использовать для восстановления в случае их потери или повреждения. Оно является важной частью кибербезопасности, поскольку позволяет защитить данные от различных угроз, таких как: несанкционированное получение конфиденциальной информации — это персональные сведения, финансовые данные или коммерческая информация; нелегальный доступ к компьютерной системе или сети. Мошенники могут использовать этот доступ для изъятия данных, распространения вредоносного ПО или нарушения работы систем [1].

Технические сбои — такие как поломка оборудования или программного обеспечения могут привести к потере данных. Частота резервного копирования данных зависит от важности ваших данных и вероятности их потери или повреждения. В целом, рекомендуется делать резервное копирование данных как минимум раз в неделю. Если ваши данные очень важны, вы можете делать резервное копирование данных ежедневно или даже несколько раз в день. Резервные копии данных можно хранить на локальном устройстве, таком как жесткий диск или внешний жесткий диск, или в облачном хранилище. Локальное хранилище является более надежным, но оно может быть менее доступным, чем облачное хранилище. Облачное хранилище является более доступным, но оно может быть менее надежным, чем локальное хранилище. Резервное копирование данных является важным шагом для защиты информации от различных угроз. Следуя приведенным выше советам, можно создать надежную систему резервного копирования данных, которая поможет защитить данные в случае их потери или повреждения.

Сегодня, в условиях широкой доступности интернета и стремительного развития средств связи, существует очень заметный разрыв в ожиданиях студентов и теми возможностями, которые могут предложить им учреждения высшего образования (вузы) России. При этих условиях формы и методы образовательной деятельности в отечественных вузах должны постоянно обновляться в зависимости от информационных потребностей и технологического развития общества. В то же время, не последнее место в этом процессе должно занимать обеспечение информационной и кибербезопасности как образовательных материалов и другой информации ограниченного доступа, так и самой ИТ инфраструктуры от случайных или направленных атак. Реализация указанных задач осложняется тем, что вузы России переживают сейчас период адаптации не только к объективным процессам информационного общества, но и к новым социально-политическим условиям с разноплановыми проявлениями конкурентной борьбы [2].

Список источников

1. Кибербезопасность в образовании: как защитить учащихся и образовательные организации / А. Тачмухаммедов, И. Ашыров, М. Гельдыева, М. Мамметдурдыев // Всемирный ученый. 2023. № 7. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-obrazovanii-kak-zaschitit-uchaschihsya-i-obrazovatelnye-organizatsii (дата обращения: 09.04.2024).

2. Технология обеспечения информационной и кибербезопасности в учреждениях высшего образования / А. С Олейник [и др.] // Управление образованием: теория и практика. 2022. № 5 (51). URL: https://cyberleninka.ru/article/n/tehnologiya-obespecheniya-informatsionnoy-i-kiberbezopasnosti-v-uchrezhdeniyah-vysshego-obrazovaniya (дата обращения: 09.04.2024).