

Наумова Ирина Викторовна

учитель

МБОУ «СОШ №3 с УИОП»

г. Строитель, Белгородская область

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация: в статье рассматриваются основные проблемы информационной безопасности образовательного процесса. Автором отмечено, что проблема информационной безопасности является наиболее важной и требует тщательного рассмотрения.

Ключевые слова: информационная безопасность, угрозы, информационная защита.

С развитием научно-технического прогресса, информационные технологии применяются практически во всех сферах человеческой деятельности. Современное поколение не может представить свою жизнь без них, а именно без социальных сетей, интернет-магазинов, онлайн-сервисов – все это является средствами коммуникаций и доступ к ним потенциально уязвим. Именно поэтому проблема информационной безопасности является наиболее важной и требует тщательного рассмотрения.

Информационная безопасность представляет собой защиту от доступа сторонних лиц, способных нанести вред чужим данным. Проблема защиты персональных данных является междисциплинарной, особенно когда касается она образовательного процесса, где основным участниками являются подрастающее поколение. За последнее десятилетие не только молодые люди становятся жертвами потери своих персональных данных, но и другие возрастные группы, являющиеся пользователями сети Интернет [1].

Использование глобальной сети Интернет влечет за собой различные риски, среди которых:

- развитие Интернет зависимости;

– компьютерная тревожность, которая может приводить к стрессовым ситуациям;

– технократизация процесса мышления.

Внедрение информационных технологий в образовательные учреждения предоставляют ряд преимуществ, а именно позволяют вести электронные журналы, следить за успеваемостью обучаемых, за успешностью работы педагогического состава, вести финансовый учет, административную деятельность. На сегодняшний день, уровень защиты данных информационных систем образовательных учреждений критически низок.

Основные причины недостаточной информационной безопасности являются [4]:

– работа на основе устаревших, небезопасных платформах. Проблемы нарушения информационной безопасности можно легко определить. Устаревшая платформа для работы уже заведомо является небезопасной. В данном случае необходимо срочное обновление, либо проведение работ устранения уязвимых пробелов;

– часто возникают проблемы, связанные с потерей либо уничтожением данных, из-за использования пиратского программного обеспечения. В основном, это взломанные программы, не требующие ключа активации. Но многие такие программы часто содержат вирусы, троянские коды, которые способны открыть доступ к персональным данным любого пользователя;

– многие организации работают в сети Интернет, используя при этом открытое соединение. Для того, чтобы избежать проблемы с потерей данных, необходимо работать на основе зашифрованного соединения.

Информационная безопасность для образовательных учреждений заключается в разграничении информации, то есть ученик в рамках школы, пользуясь сетью Интернет не должен столкнуться с информацией, способной негативно повлиять на него [3]. Мало внимания уделяется проблеме социальных сетей, которая, уже сегодня, заменяет живое общение. Виртуальное пространство, хоть и лишено близости друг с другом людей, но не исключает проблемы запугивания,

угроз, растления, особенно если этому воздействию подвергается психически не окрепшая личность.

Выделим основные угрозы информационной безопасности, наиболее проявляющиеся в образовательных учреждениях:

– несанкционированный доступ к данным, который заключается в подмене достоверной информации, хищении данных, например, содержания экзаменационных билетов, личных данных обучающихся;

– фильтрация доступной информации. То есть предоставление доступа только к полезным источникам информации. Запрет к сайтам, несущим порнографический характер, пропаганда наркотиков, алкоголя, экстремистской идеологии;

– кибертерроризм: подразумевает повреждение и разрушение действующих автоматических систем. Следует отметить, что данная угроза встречается крайне редко, так как образовательные учреждения не содержат информации, соответствующей целям кибератак.

К одним из способов обеспечения информационной безопасности образовательного учреждения можно отнести постоянный контроль образовательных систем. Многие учреждения не считают необходимым ставить пароли высокого уровня сложности, и ставят простые, легкие для запоминания, а также доступные для взлома. Данная проблема присуща не только образовательным учреждениям [2].

В том случае, когда пользователь не знаком с правилами информационной гигиены, он с легкостью может стать жертвой мошенников. Именно поэтому, в обучении информатики, существуют разделы, связанные с рассмотрением вопросов информационной безопасности и сохранности своих личных данных. Также, при повышении квалификации преподавательского состава должны быть включены разделы на информирование о необходимости контроля защиты данных.

В качестве оптимального способа информационной защиты, целесообразно создание единой платформы работы, за безопасностью которой следили бы высококвалифицированные специалисты. Однако данный вариант требует огромных затрат, и поэтому образовательным учреждениям приходится самостоятельно решать возникающие проблемы.

В настоящее время информационные технологии применяются активно в любой профессиональной деятельности. Для современного ученика доступ к огромному количеству информации так же естественен, как и очное общение.

Сегодня, разработан ряд законов, цель которых заключается в ограничении распространяемой информации в Интернете, что вызвало массу недовольств у более взрослого населения, чья деятельность связана напрямую с работой в глобальной сети.

Таким образом, обеспечение информационной безопасности важнейший аспект образовательного процесса, значимость которого с каждым годом только возрастает. В процессе обучения, даже младшие школьники должны быть проинформированы о проблемах информационной безопасности и кибератаках. Обучающиеся должны понимать, какую информацию можно доверить своим гаджетам, различным сайтам и приложениям. Тщательно продуманный подход к решению данной проблемы, способен разработать наиболее сильную информационную безопасность для общества.

Список литературы

1. Алиева М.Ф. Информационная безопасность как элемент информационной культуры / М.Ф. Алиева // Вестник АГУ. – 2012. – 4 (108). – С. 47 – 52.
2. Асадулаева С.А. Национальная безопасность и её влияние на личность / С.А. Асадулаева // Мир науки, культуры, образования. – 2017. – 4 (65). – С. 228 – 229. – EDN ZEJHSL
3. Каберник В.В. Обеспечение безопасности образовательной среды / В.В. Каберник, О.А. Тимофеева // Вестник МГИМО Университета. – 2015. – 4 (43). – С. 119–129. – EDN UDUNMV
4. Литвинова А.В. Оценка информационной безопасности образовательной среды учащимися и родителями / А.В. Литвинова, А.С. Блинова // European Social Science Journal. – Т. 1. – 2013. – 12. – С. 149 – 152. – EDN SDJWFH
5. Кузина Н.Н. Информационная безопасность как условие успешной социализации современной молодежи / Н.Н. Кузина // Материалы III Международной научной конференции. – 2017. – С. 203–207. – EDN YTWKFJ