www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2021.4.3

УДК 81:004
ББК 81.006.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБУЧАЮЩИХСЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент, кафедра методики преподавания математики и физики, ИКТ, Волгоградский государственный социально-педагогический университет
yarikov_vg@mail.ru
просп. им. В. И. Ленина, 27, 400131 г. Волгоград, Российская Федерация

Аннотация. Проведен анализ существующих угроз в сфере информационной безопасности и опасностей использования интернет-ресурсов, социальных сетей. Показано, что деятельность в области информационной безопасности является одним из приоритетных условий развития сферы образования в ближайшем будущем.

Ключевые слова: информационная безопасность, интернет-ресурсы, социальные сети, образовательные организации, информационные технологии.

Актуальность вопроса обусловлена значительными изменениями в социальной, политической и экономической жизни современного общества под влиянием процесса массового использования информационных технологий и активным внедрением дистанционных технологий обучения в систему образования.

Большое значение имеют перемены, спровоцированные масштабным внедрением информационных технологий в сферу образования. Образовательные учреждения перестают быть местом получения готовых и общепринятых знаний, они становятся местом коммуникаций и информационного обмена обучающихся с окружающим миром и взаимодействия с информационными системами, обеспечивающими образовательный процесс. В связи с этим одной из основных задач образования становится задача информационной безопасности обучающихся в образовательных учреждениях всех уровней.

Важным требованием обеспечения деятельности образовательного учреждения на сегодняшний день является поддержание высокого уровня информационной безопасности. Причем вопросы информационной безопасности (ИБ) в образовательных организациях имеют свою специфику. Информационная безопасность в системе образования в целом и в каждом конкретном образовательном учреждении должна представлять собой системный комплекс мероприятий, направленных на реализацию двух основных задач. Помимо защиты информационной системы учреждения, баз данных, как внутренних, так и внешних, и предотвращения хакерских атак, также важно оградить обучающихся от любых проявлений незаконной пропаганды и попыток манипулирования. Вследствие этого построение системы информационной безопасности в образовательных учреждениях должны обеспечивать квалифицированные специалисты, оснащенные современным программно-техническим комплексом.

ИБ в образовательной организации

Целью работы службы или отдела информационной безопасности в современной образовательной организации всех уровней,

в соответствии с действующим законодательством РФ, должна быть защита сведений и данных, которые относятся к указанным ниже группам:

– персональные данные и сведения об обучающихся, педагогах и иных сотрудниках образовательной организации, а также доступ к документам для служебного пользования;

– обучающие программы, базы данных, применяемые для обеспечения учебного процесса, медиа продукция и авторские разработки, защищаемые законом как интеллектуальная собственность.

Действия правонарушителей могут привести к утере, краже или искажению упомянутых данных, которые используются для обеспечения образовательного процесса.

В обязанности сотрудников отдела информационной безопасности в организации должны входить:

– обеспечение целостности защищаемых данных;

– обеспечение непрерывного доступа к информации для лиц с соответствующими правами;

– обеспечение конфиденциальности сведений, например, персональных данных и предотвращение доступа к ним со стороны злоумышленников.

Необходимо отметить особенности используемого ПО для работы с персональными данными и документооборота в организациях довузовского и высшего образования. В системе довузовского образования централизованно используется удаленная система «Сетевой город. Образование». В системе высшего образования используется более широкий список программ, в основном продукция фирмы «1С».

В «Сетевом городе» для защиты персональным данных используются ЭПЦ, системы криптозащиты и аттестация конкретных АРМ для работы с закрытой информацией и помещений для них.

В высшем образовании доступ к персональным данным имеет меньшую защиту, в основном пароли доступа к соответствующим программам и ограничение работы с программами на территории вуза. При этом вузы являются субъектами критической инфраструктуры и могут заниматься технологиями двойного назначения.

Угрозы информационной безопасности

Особенностью обеспечения ИБ в образовательных учреждениях в настоящее время является состав отличительных угроз. К ним относится не только возможность хищения или деформации данных третьими лицами, но также осознанная или неосознанная разрушительная деятельность обучающихся. Обучающиеся могут заразить информационную систему учреждения вирусными программами или повредить компьютерную технику учреждения.

Угрозам осознанного или неосознанного деструктивного воздействия могут подвергаться следующие группы объектов образовательного учреждения:

– программное обеспечение;

– данные, которые хранятся в информационной системе организации;

– данные, хранящиеся во внешней информационной системе, с которой взаимодействует организация;

– обучающиеся, которые могут подвергаться стороннему информационному воздействию;

– сторонние интернет-ресурсы, используемые в образовательном процессе и социальных коммуникациях;

– воздействие сторонних интернет-ресурсов, используемых в образовательном процессе и социальных коммуникациях;

– оргтехника образовательной организации.

Угрозы информационной безопасности образовательного учреждения могут носить не умышленный и умышленный характер. Угрозы первого характера в большинстве случаев имеют временный характер, и с ними справляется персонал организации соответствующих отделов.

Значительно более опасными угрозами для информационной безопасности организации являются угрозы умышленного характера. Обычно результаты их осуществления невозможно предвидеть. Умышленные угрозы могут исходить от обучающихся, работников организации, хакеров. Наиболее уязвимым объектом для атаки являются сети с распределенными территориально элементами. Злоумышленники могут достаточно про-

сто нарушать информационный обмен между такими удаленными элементами сети или нанести более серьезный ущерб системе. Также внешние атаки на информационные ресурсы образовательной организации или используемые организацией иные информационные ресурсы, могут предприниматься для воздействия на сознание обучающихся, например, через социальные сети. Наиболее актуальная угроза в настоящее время это возможность вовлечения обучающихся в деструктивную, криминальную, террористическую деятельность или в объединения преследующие суицидальные цели.

Отдельно в качестве угрозы информационной безопасности необходимо упомянуть так называемый человеческий фактор. Какие бы не предпринимались усилия по обеспечению информационной безопасности, легкомысленное отношение к данному вопросу сводит все усилия на нет. Наиболее типичными действиями большинства пользователей, нарушающими требования информационной безопасности являются:

– простые пароли;

– пароли, которые на изменяются длительное время, иногда годами;

– неконтролируемый доступ к автоматизированным рабочим местам;

– неконтролируемое использование внешних носителей, часто распространяющих компьютерные вирусы;

– нарушение регламентов использования электронных цифровых подписей;

– общая компьютерная неграмотность ряда сотрудников;

– размещение или передача в социальных сетях закрытой информации;

– негативное воздействие на сознание через социальные сети.

Меры защиты

Современные технологии в области информационной безопасности, доступные образовательным организациям, которые прописаны в том числе и на законодательном уровне, предусматривают организацию защиты по следующим направлениям:

– нормативно-правовое;

– морально-этическое;

– административно-организационное;

– просветительское;

– техническое.

Рассмотрим подробнее меры защиты, предпринимаемые на каждом из этих уровней.

Нормативно-правовые способы защиты

Основными федеральными документами, определяющим степень угроз и меры обеспечения информационной безопасности в образовательных учреждениях, являются Федеральный закон «О персональных данных» [3] и «Национальная стратегия действий в интересах детей» [2]. Данные документы предусматривают комплекс мер, направленных на защиту персональных данных и сознания обучающихся от агрессивного воздействия внешней информационной среды. Меры по защите информационной инфраструктуры организации и информационных баз данных имеют второй уровень приоритетности.

Законодательством определяются данные в информационной системе образовательной организации, которые должны быть защищены от несанкционированного доступа. К числу таких данных относятся:

– персональные обучающихся и сотрудников;

– служебная, профессиональная, коммерческая тайна;

– иная конфиденциальная информация.

Порядок обеспечения безопасности персональных данных регламентируется соответствующими законодательными актами Российской федерации, а также нормативной документацией каждой конкретной образовательной организации.

Морально-этические средства обеспечения информационной безопасности

В сфере образования система морально-этических норм ценностей имеет особое, отличное от остальных сфер жизни общества значение. Она служит основой для выработки стратегий воспитательной работы и профилактической деятельности образовательного учреждения, направленных на защиту обу-

чающихся от информации противозаконного, этически некорректного и иного деструктивного характера. Целесообразно подключать к такой работе и сотрудников органов правопорядка для организации комплексной работы в этой области. Воспитательная деятельность в образовательных организациях осуществляется согласно утвержденному плану воспитательной работы организации, что позволяет включить в него соответствующие мероприятия и сделать работу системной и регулярной.

Меры административно-организационного характера

Система административно-организационных мер строится на базе внутренних регламентов и правил, на которых базируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

– должностные инструкции;

– внутренние методики по ИБ;

– перечни не подлежащих передаче данных;

– регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными правилами и регламентами информационной безопасности образовательной организации должны определяться:

– порядок доступа обучающихся к учебным местам, оборудованным компьютерной техникой на время занятий;

– порядок доступа сотрудников к автоматизированным рабочим местам;

– доступ к локальной сети организации и сети интернет;

– выполнения иных работ сотрудниками в информационной системе;

– меры по предотвращению доступа обучающихся к определенным ресурсам, использование систем контент фильтрации;

– блокирование использования обучающимися своих носителей информации и т. д. [1].

Просветительские меры

Большое значение в области обеспечения информационной безопасности имеют просветительские, иначе их можно назвать профилактические, меры. Постоянная разъяснительная работа среди сотрудников и обучающихся о необходимости защиты информации, персональных данных позволит повысить уровень культуры информационной безопасности и воспринимать задачи информационной безопасности не как помеху в работе, а как важный элемент своей работы и повседневной жизни.

Отдельно необходимо отметить работу, направленную на предотвращение небезопасного использования сетевых ресурсов в целом и социальных сетей в частности. Активность обучающихся и преподавателей в социальных сетях часто приводит к негативным последствиям, связанным с использованием персональных данных злоумышленниками, причем эти данные пользователи нередко размещали в социальных сетях сами.

К числу просветительских мер относятся:

– регулярная просветительная работа;

– проведение обучающих семинаров;

– прохождение сотрудниками профильных курсов повышения квалификации.

Плановое проведение подобных мероприятий позволит не только повысить уровень информационной безопасности образовательного учреждения, но и уровень личной информационной безопасности сотрудников и обучающихся, их позитивное личностное развитие.

Технические меры

Технические меры защиты предусматривают использование специализированного программного обеспечения, прежде всего комплекс специальных программ для электронного документооборота и работы с персональными данными. Это может быть программное обеспечение собственной разработки или от сторонних производителей из реестра отечественного ПО. Реестр создан в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации» [4] в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации.

Также в организациях системы образования можно рекомендовать использовать

DLP и SIEM-системы, которые своевременно обнаруживают различные угрозы информационной безопасности и обеспечивают эффективную борьбу с ними. К сожалению, часто в образовательных организациях, которые в большинстве своем являются бюджетными, нет невозможности использования специализированного программного обеспечения в силу бюджетных ограничений, поэтому можно рекомендовать использовать антивирусы, системы контент фильтрации и другие виды специализированного программного обеспечения, имеющие соответствующие сертификаты ФСТЕК.

Анализ существующих угроз в сфере информационной безопасности и опасностей использования интернет-ресурсов, в особенности социальных сетей, показал, что деятельность в области информационной безопасности является одним из приоритетных условий ее развития сферы образования в ближайшем будущем.

Исследования в области культуры ИБ открывают перспективу для дальнейшего изучения проблемы обеспечения информационной безопасности в образовательных учреждениях в контексте культуры безопасности человека XXI века, идей открытого образования и методик информатизации образования.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность в образовательной организации : Блог // Smart-SoftTeam. – Электрон. дан. – Режим доступа: https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii/ (дата обращения: 01.11.2021). – Загл. с экрана.

2. Указ Президента РФ от 1 июня 2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012–2017 годы». – Электрон. дан. – Режим доступа: https://base.garant.ru/70183566/#block_1000 (дата обращения: 02.12.2021). – Загл. с экрана.

3. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 02.12.2021). – Загл. с экрана.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.12.2021). – Загл. с экрана.

REFERENCES

1. Informacionnaya bezopasnost' v obrazovatel'noj organizacii: Blog [Information Security in an Educational Organization. Blog]. *Smart-SoftTeam*. URL: https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii (accessed 1 November 2021).

2. *Ukaz Prezidenta RF ot 1 iyunya 2012 g. № 761 «O Nacional'noj strategii dejstvij v interesah detej na 2012–2017 gody»* [Decree of the President of the Russian Federation No. 761 Dated June 1, 2012 "On the National Strategy of Actions in the Interests of Children for 2012–2017"]. URL: https://base.garant.ru/70183566/#block_1000 (accessed 2 December 2021).

3. *Federal'nyj zakon «O personal'nyh dannyh» ot 27.07.2006 № 152-FZ (poslednyaya redakciya)* [Federal Law No. 152-FZ Dated July 27, 2006 "On Personal Data" (Last Revision)]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801 (accessed 2 December 2021).

4. *Federal'nyj zakon «Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii» ot 27.07.2006 № 149-FZ (poslednyaya redakciya)* [Federal Law No. 149-FZ Dated July 27, 2006 "On Information, Information Technologies and Information Protection" (Last Revision)]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798 (accessed 2 December 2021).

INFORMATION SECURITY OF STUDENTS IN AN EDUCATIONAL ORGANIZATION

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Methods of Teaching Mathematics and Physics, ICT,
Volgograd State Social and Pedagogical University
yarikov_vg@mail.ru
Prosp. Lenina, 27, 400131 Volgograd, Russian Federation

Abstract. The relevance of the issue is due to significant changes in the social, political and economic life of modern society under the influence of the process of mass use of information technologies and the active introduction of distance learning technologies into the education system. An important requirement for ensuring the activities of an educational institution today is to maintain a high level of information security. Moreover, the issues of information security in educational organizations have their own specifics. The analysis of existing threats in the field of information security and the dangers of using Internet resources, social networks is carried out. It is shown that the activity in the field of information security is one of the priority conditions for its development in the field of education in the near future. Information security in the education system as a whole and in each specific educational institution should be a systematic set of measures aimed at the implementation of two main tasks. In addition to protecting the institution's information system, databases, both internal and external, and preventing hacker attacks, it is also important to protect students from any manifestations of illegal propaganda and manipulation attempts. As a result, the construction of an information security system in educational institutions should be provided by qualified specialists equipped with a modern software and hardware complex.

Key words: information security, Internet resources, social networks, educational organizations, information technologies.