УДК 37.014 DOI: 10.18720/HUM/ISSN 2227-8591.22.6

О.А. Козлов, Л.А. Гузикова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК УСЛОВИЕ ДЕЯТЕЛЬНОСТИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

КОЗЛОВ Олег Александрович – доктор педагогических наук, профессор, Институт управления образованием Российской академии образования,
ул. Макаренко, 5/16, строение 1Б, Москва, 105062, Россия; e-mail: olekozlov@yandex.ru

KOZLOV Oleg A. – Institute of Education Management of the Russian Academy of Education,
ul. Makarenko, 5/16, building 1Б, 105062, Moscow, Russia; e-mail: olekozlov@yandex.ru

ГУЗИКОВА Людмила Александровна – доктор экономических наук, профессор, Высшая школа государственного и финансового управления, Институт промышленного менеджмента, экономики и торговли, Санкт-Петербургский политехнический университет Петра Великого,
ул. Политехническая, 29, Санкт-Петербург, 195251, Россия; e-mail: guzikova@mail.ru

GUZIKOVA Liudmila A. – Peter the Great St. Petersburg Polytechnic University. Politekhnicheskaya ul., 29, St. Petersburg, 195251, Russia; e-mail: guzikova@mail.ru

Информационная среда современного общества охватывает все сферы человеческой деятельности и включает в себя колоссальный объем информации. Вопросы информационной безопасности чаще всего рассматриваются в контексте национальной безопасности, однако следует учитывать, что одним из наиболее активных потребителей и генераторов информации является сфера образования, где формируется интеллектуальный и нравственный потенциал будущих поколений. Эффективность образовательной системы в значительной мере зависит от эффективности потребления и генерации информации, что позволяет ставить вопрос об ограждении обучаемых от информации, способной нанести ущерб личности обучаемого и спровоцировать деструктивные последствия. В статье проанализированы факторы риска и угрозы информационной безопасности в образовательных учреждениях, дана трактовка понятия информационной безопасности личности, предложены цели создания системы информационной безопасности в образовательной организации, дана классификация угроз информационной безопасности и соответствующих уровней опасности. Авторами обоснована необходимость встраивания системы обеспечения информационной безопасности в деятельность образовательных учреждений. В качестве социально-педагогического решения по обеспечению информационной безопасности обучаемых предложено включение в деятельность педагогических и управленческих кадров компетентности в области информационной безопасности как компонента профессиональной подготовки.

ИНФОРМАЦИОННО-КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ; ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ; НЕГАТИВНАЯ ИНФОРМАЦИЯ; ИНФОРМАЦИОННЫЕ УГРОЗЫ

Ссылка при цитировании: Козлов О.А., Гузикова Л.А. Информационная безопасность как условие деятельности образовательных организаций // Вопросы методики преподавания в вузе. 2017. Т. 6. № 22. С. 43–50. DOI: 10.18720/HUM/ISSN 2227-8591.22.6

Введение. В современном обществе информационная сфера представляет собой системообразующий фактор, определяющий все происходящие в жизни общества процессы и поведение членов общества как участников этих процессов. Информационная среда оказывает активное влияние на все составляющие безопасности государства – политическую, экономическую, оборонную и другие [1]. Она оказывает мощнейшее воздействие и на состояние образовательной системы. Растущая зависимость от информационно-коммуникационных технологий во всех областях человеческой жизни привела к уязвимости, которые необходимо надлежащим образом определить, тщательно проанализировать, устранить или уменьшить. Все соответствующие субъекты – государственные органы, частный сектор или отдельные граждане – должны признать эту общую ответственность, принять меры для защиты и при необходимости обеспечить скоординированные меры по укреплению безопасности в информационном пространстве.

О значимости информационной безопасности свидетельствует, в частности, тот факт, что в настоящее время в мире насчитывается более 500 стандартов и нормативных документов по информационной безопасности. В России действует около 40 ГОСТов и примерно 70 нормативных актов [2].

Бурное развитие современных информационных и коммуникационных технологий (ИКТ), которым сопровождается формирование информационного общества, сопряжено с фронтальным воздействием на физическое, психическое, и интеллектуальное развитие подрастающего поколения, на формирование личности и ее нравственного облика [3]. Необходимо отметить, что сегодня учебно-воспитательный процесс в образовательных учреждениях различного типа происходит в рамках сетевого взаимодействия всех участников этого процесса в условиях информационно-образовательной среды.

Основные положения и результаты. Под информационно-образовательной средой, следуя словарю [4], мы будем понимать совокупность условий, обеспечивающих контакт и взаимодействие пользователя с информационным ресурсом (в том числе, распределенным) с использованием интерактивных средств информационных и коммуникационных технологий, взаимодействующих с ним как с субъектом информационного обмена и личностью.

Организация взаимодействия участников учебно-воспитательного процесса представлена на рис. 1.

Очевидно, что при сетевом взаимодействии через отрытые каналы связи все участники взаимодействия могут стать как объектом, так и источником угроз информационной безопасности образовательного учреждения и личности. Как указывается в статье авторов А.Н. Ищенко, А.Н. Прокопенко, А.А. Страхова [5], утверждение о том, что «Интернет – это свободное киберпространство», никогда не было истиной. Отсутствие единого владельца у Интернета действительно нет, однако администрирование ключевых ресурсов и управление основными функциями осуществляется кругом организаций, деятельность которых подконтрольна.

Молодые люди, как правило, проводят в сети больше времени, чем взрослые. Отмечается также более высокий уровень использования Интернета учащейся молодежью, по сравнению с теми, кто не учится. Для молодых людей во всем мире социальные сети и созданные пользователями материалы, такие как блоги, стали ключевыми факторами Интернет-поглощения.

Интернет имеет большой потенциал в качестве средства расширения возможностей учащихся, помогая им находить необходимую и/или интересующую их информацию. В настоящее время распространено мнение, что Интернет может

иметь реальное значение в образовательном процессе. Волна инноваций в области образования связана с расширением использования возможностей Интернет для обеспечения большей гибкости и персонализации учебного процесса по сравнению с традиционными способами его организации.

Для глобальной информационной среды характерны всеобщая компьютеризация и информатизация, тотальное внедрение информационных и коммуникационных технологий во все сферы жизни и деятельности, включая сферу образования. Обратной стороной доступности информации становится повышение опасности для детей и учащейся молодёжи, возникновение новых факторов риска, угроз негативного информационного воздействия на всех участников образовательного процесса. Наименее защищенными в таких условиях оказывается подрастающее молодое поколение, которое еще не успело выработать строгое мировоззрение, четкую жизненную позицию. Таким образом, в условиях общества глобальной коммуникации доступность информации создает проблему информационной безопасности (ИБ) личности [6].

Несмотря на целый ряд достоинств ИОС (доступ пользователей к учебному контенту в любое время из любой точки, индивидуализация обучения и контроля, быстрое распространение передовых образовательных практик и т. д.), следует отметить, что актуальной является проблема обеспечения информационной безопасности не только субъектов образовательного процесса, но и самой образовательной организации.

Процесс управления образовательной организацией, ориентированный на достижение плановых показателей качества, должен быть направлен, среди прочего, на создание и поддержание на необходимом уровне инфобезопасной среды образовательной организации как условия обеспечения информационной безопасности всех субъектов образовательного процесса. Представляется, что инфобезопасная среда образовательной организации должна обеспечивать [7]:

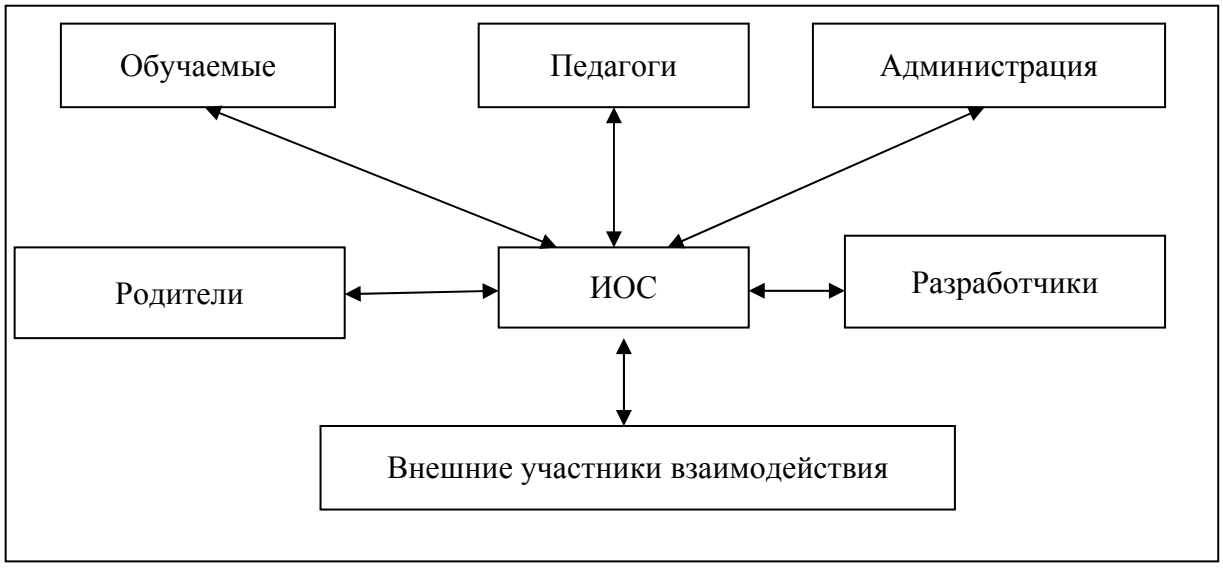

Рис. 1. Структура сетевого взаимодействия всех участников учебно-воспитательного процесса в условиях ИОС.

– защиту обучающихся от информации, которая может причинить вред их здоровью и развитию;

– защиту информационных ресурсов и систем образовательной организации;

– защиту персональных данных всех участников образовательного процесса.

Для обеспечения эффективной комплексной защиты в первую очередь необходимо рассмотреть и проанализировать деструктивные факторы, представляющие угрозу ИОС. К факторам риска информационной среды, представляющим потенциальную опасность для детей и молодежи, следует отнести наличие в информационной среде [8, с. 196–201]:

1) противоправного контента, вредоносной информации, оказывающей воздействие на нравственное развитие и ценностные ориентиры молодого поколения;

2) специфических элементов, целенаправленно изменяющих психофизиологическое состояние обучающихся;

3) контента манипулятивного характера, способного дезориентировать обучаемого, ограничить его возможности в условиях слабой правовой подготовки и возрастных особенностей;

4) возможностей несанкционированного использования персональных данных и/или разглашения конфиденциальных сведений, обусловленных трудностями реализации механизмов охраны этих сведений, успехами в области миниатюризации средств скрытного сбора и передачи информации.

Необходимо отметить, что современный мир отвергает концепцию абсолютной безопасности, заменяя ее концепцией приемлемого допустимого риска. Достижение абсолютной безопасности в процессе жизнедеятельности невозможно, так как всегда существует некоторый остаточный риск. Исходя из такого представления, следует понимать информационную безопасность личности как приемлемый уровень риска. Приемлемый риск как «системная» характеристика является неснижаемым. Однако реальный уровень риска может быть не только неприемлемым, но и чрезмерным, то есть представляющим опасность для жизнедеятельности [9].

Актуальность проблемы защиты информационного пространства и обеспечения информационной безопасности непосредственно обусловлена реальными и потенциальными угрозами и рисками информационной безопасности. Уровень и масштабы этих угроз и рисков за последнее десятилетие возросли многократно, а результаты их воздействия приобрели исключительно опасный характер [10].

В сфере обеспечения информационной безопасности одним из ключевых понятий является понятие угрозы. Под угрозой в общем случае под угрозой понимается возможное событие, явление, действие или процесс, которое потенциально способно нанести ущерб чьим-либо интересам. Угроза объекту информационной безопасности это совокупность факторов и условий, которые возникают в процессе взаимодействия различных объектов или их элементов и способны оказать негативное воздействие на конкретный объект информационной безопасности.

В научной литературе существуют различные классификации угроз информационной безопасности [11, 12]. Негативные воздействия различаются по характеру наносимого вреда, а именно: по степени изменения свойств объекта безопасности и возможности ликвидации последствий проявления угрозы [12, 13].

Можно выделить четыре уровня опасности для субъектов образовательного процесса, связанной с угрозами информационной безопасности (табл. 1).

Таблица 1

Уровни и проявления угрозы информационной безопасности

Уровень угрозы	Возможные проявления реализации угрозы для субъектов образовательного процесса
низкий	незначительные негативные последствия
средний	негативные последствия
высокий	значительные негативные последствия
критический	потеря жизни или здоровья

Тип информационного опыта, получаемый учащимися в рамках сетевого взаимодействия, является важным фактором, определяющим типы рисков, которым они подвергаются, и, следовательно, типы защиты, которая может быть наиболее эффективной.

Информационным угрозам подвергаются не только субъекты ИОС как элементы этой системы, но и связи между ними. Учитывая, что в рамках ИОС происходит взаимодействие ее субъектов, можно рассматривать информационные воздействия с точки зрения угрозы учебному процессу, возможности его реализации и достижению его целей.

Методология управления рисками должна включают четыре основных шага оценки риска:

1. инвентаризация сетевых ресурсов, включенных в сферу оценки;
2. идентификация угроз, связанных с этими активами;
3. категорирование вероятности и потенциальных результатов реализации угроз для субъектов ИОС и связей;
4. определение средств контроля, необходимых для снижения выявленных рисков до приемлемого уровня.

Анализ угроз и рисков создает предпосылки для формирования компетентности педагогических работников и управленческих кадров в области ИБ посредством освоения ряда дополнительных специальных компетенций. Содержание педагогических воздействий на каждом этапе обучения должно определяться в зависимости от актуальных угроз информационной безопасности. Необходимо также разработать условия безопасного использования соответствующих образовательных информационных сервисов.

Особенность обучения информационной безопасности состоит в том то, что изучения только правового, организационного и технического обеспечения информационной безопасности недостаточно для эффективного противодействия угрозам сетевой информационной среды. Необходимо воспитать нравственность и ответственность за использование информации, которая может причинить ущерб не только личности, неумело с ней обращающейся, но и другим участникам информационных процессов [9]. Противодействием угрозам информационной безопасности должно стать обучение позитивным и ответственным формам онлайн-поведения.

Под информационной безопасностью личности следует понимать такое состояние и условия жизнедеятельности личности, при которых минимизирована или отсутствует угроза нанесения вреда личному информационному пространству и информации, которой обладает индивид [6].

По результатам анализа современных исследований по проблемам информационной безопасности можно сделать вывод, что в настоящее время в российской образовательной системе отсутствует комплексный подход к формированию системы информационной безопасности. Отдельные организационно-педагогические мероприятия и действия, ориентированные на обеспечение информационной безопасности личности, можно рассматривать только как предпосылки к разработке и принятию педагогическим сообществом более широкого комплекса мер.

В качестве целей создания системы информационной безопасности в образовательной организации следует привести:

1) защиту обучающихся, педагогов, их прав и интересов, а также имущества от опасных воздействий, генерируемых информационной средой;

2) обеспечение эффективного функционирования и развития образовательной организации;

3) снижение ущерба от негативных воздействий угроз информационной безопасности, снижение вероятности проявления угроз и последствий реализации рисков;

4) улучшение качества жизни, повышение благополучия учащихся и педагогов (за счет снижения психологических расстройств, смертности, повышения сохранности здоровья, снижения риска потери или хищения информации).

Согласно исследованиям Дубовой Ю.С**.** [14] комплекс мер по обеспечению информационной безопасности должен включать:

- правовые (законодательные) меры;
- технологические меры;
- организационные (административные и процедурные) меры;
- технические (физические, аппаратные и программные) средства;
- морально-этические нормы;
- средства мониторинга эффективности.

При создании системы информационной безопасности в образовательной организации необходимо учитывать ключевые характеристики информационной среды, в рамках которой реализуется сетевое взаимодействие. Такая среда обладает следующими свойствами:

- она создана и поддерживается для конкретных целей;
- она является динамичной;
- она является быстрой;
- она относительно безгранична;
- она имеет низкие входные барьеры;
- она быстро растет;
- ее можно рассматривать с позиций различных структур, которые неизбежно формируют представления о соответствующем поведении и ценностях [15].

Выводы. Информационная безопасность относится к механизмам, которые защищают ИОС от негативного воздействия, исходящего из сетевого пространства. Она не должна сводиться к простому техническому контролю аппаратных и программных средств и сетевых ресурсов, ее следует понимать как исследование и практику защиты субъектов ИОС во всех ее формах.

Проблема обеспечения информационной безопасности ИОС характеризуется острой необходимостью и неотложностью. Социально-педагогическое решение проблемы информационной безопасности состоит, по нашему мнению, в обязательном включении в деятельность педагогических и управленческих кадров такого компонента профессиональной подготовки как компетентность в области информационной безопасности. Педагогическое воздействие должно быть направлено не только на привитие знаний, умений и навыков работы с информацией, но также на формирование опыта деятельности по защите от негативной информации в профессиональной и управленческой деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. **Алексеева Е.В.** Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. № 4 (46). С. 97-103. ISSN: 1813-6230

2. **Филяк П.Ю.** Информационная безопасность и комплексная система безопасности:

анализ, подходы // Информация и безопасность. 2016. Т. 19. № 1. С. 72–79. ISSN: 1682-7813

3. **Роберт И.В.** Перспективные научные исследования, определяющие развитие информатизации образования // Педагогическое образование в России. 2014.№4. С. 199-204. ISSN: 2079-8717

4. Толковый словарь терминов понятийного аппарата информатизации образования. – М.: ИИО РАО, 2009. – 96 с. ISBN: 978-5-94774-845-1

5. **Ищенко А.Н., Прокопенко А.Н., Страхов А.А.** Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. № 2. С. 55-62. ISSN: 1819-7426

6. **Бочаров М.И., Козлов О.А., Симонова И.В.** Анализ современной подготовки педагогических кадров в области информационной безопасности // Инновации на основе информационных и коммуникационных технологий. 2012. №1. С. 29–32. ISSN: 2226-6690

7. **Мухаметзянов И.Ш.** Методические рекомендации по предотвращению негативных последствий использования компьютера. М. – ИИО РАО, 2011. – 33 с.

8. **Пазухина С.В.** Ребенок за компьютером: психологические риски и экстремальные ситуации в виртуальной «жизни» младшего школьника // Ст. в сб.: Психолого-педагогические основания формирования ценности здоровья, культуры здорового и безопасного образа жизни в системе образования / Сост. и науч. ред. Н.Ю. Синягина, Е.Г Артамонова, Н.В Зайцева. – М.: АНО «ЦНПРО», 2013. – 296 с. ISBN: 978-5-905430-19-0

9. **Козлов О.А., Бочаров М.И.** Педагогико-эргономические и дидактико-методические принципы проектирования методической системы обучения студентов информационной безопасности // Ученые записки ИИО РАО. 2012. №43. С. 43-56 eISSN: 2500-4395

10. **Малюк А.А., Бочаров М.И., Козлов О.А.** Система профессионального обучения информационной безопасности в Российской Федерации // Информатика и образование. 2013. №10(249).С. 9-16. ISSN: 0234-0453

11. **Малюк А.А.** Информационная безопасность: концептуальные и методологические основы защиты информации /монография. – М.: Горячая линия – Телеком, 2004. – 280 с. ISBN: 5-93517-197-X

12. **Саттарова Н.И.** Информационная безопасность школьников в образовательном учреждении: дисс. ... канд. пед. наук: 13.00.01. – СПб., 2003. – 215 с.

13. **Козлов О.А., Козлов А.О.** Современные подходы к проблеме эффективной организации и обеспечения интегрированной защиты программного обеспечения вычислительных сетей образовательных учреждений // Ученые записки ИИО РАО. 2014. №54. С. 86–105. eISSN: 2500-4395

14. **Дубова Ю.С.** Информационная безопасность в киберпространстве // Вестник Кыргызско-Российского славянского университета. 2016.Т.16. № 4. С.154-157.ISSN: 1694-500X

15. **Nielsen S.C.** Pursuing Security in Cyberspace: Strategic and Organizational Challenges. Orbis. 2012.56(3) P.336-356

Kozlov O.A., Guzikova L.A. **Information security as requisition of educational organization activity.** The information environment of modern society covers all spheres of human activity and includes an enormous amount of information. Information security issues are most often considered in the context of national security, but it should be taken into account that one of the most active consumers and producers of information is the education sector, where the intellectual and moral potential of future generations is formed. The effectiveness of the educational system depends to a large extent on the effectiveness of consumption and generation of information, which makes it possible to raise the issue of protecting trainees from information that could damage the trainee's personality and provoke destructive consequences. Risk factors and threats to educational institutions' information security are analyzed in the article, the concept of personal information security is considered, the goals of

information security system implementing in the educational organization are proposed, classification of threats to information security and corresponding levels of danger is given. The authors justify the necessity of embedding the information security system in the activities of educational institutions. As a socio-pedagogical decision to ensure information security of trainees, it is proposed to include the competence in the field of information security into the activities of pedagogical and managerial staff.

INFORMATION AND COMMUNICATION TECHNOLOGIES; INFORMATION SECURITY; NEGATIVE INFORMATION; INFORMATION THREATS

Citation: Kozlov O.A., Guzikova L.A. Information security as requisition of educational organization activity. *Teaching Methodology in Higher Education*. 2017. Vol. 6. No 22. P. 43–50. DOI: 10.18720/HUM/ISSN 2227-8591.22.6