- УПРАВЛЕНИЕ ОБРАЗОВАНИЕМ -

Дата поступления рукописи в редакцию: 02.07.2026 г. DOI: 10.24412/2782-3830-2026-8-240-247
Дата принятия рукописи в печать: 25.07.2026 г.

АКАПЬЕВ Виктор Львович,
кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: akapevv@yandex.ru

КОВАЛЕВА Екатерина Геннадьевна,
кандидат технических наук, доцент кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: kovalevazchs@yandex.ru

БОРИСЕНКО Александр Васильевич,
кандидат физико-математических наук, старший преподаватель кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: borisenko02.94@mail.ru

НОВИКОВА Екатерина Анатольевна,
кандидат юридических наук, доцент, начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: tomchik1980@mail.ru

ПРАВОВЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ

Аннотация. *Современное общество переживает глубокую трансформацию, в основе которой лежит стремительное распространение цифровых технологий, охватывающее практически все сферы жизни человека, включая образование, досуг, профессиональную деятельность и повседневное общение. Дети школьного возраста оказываются погружены в цифровую среду значительно раньше, чем успевают сформировать устойчивые представления о безопасном поведении в ней, и именно это обстоятельство превращает вопросы их информационной безопасности в одну из наиболее острых социальных проблем современности. Прежде всего необходимо отметить неуклонный рост числа киберугроз, которым подвергаются несовершеннолетние пользователи сети Интернет. При этом возможности детей самостоятельно распознавать подобные угрозы существенно ограничены ввиду недостаточного жизненного опыта и низкого уровня цифровой грамотности. Школа как главный институт социализации объективно выступает тем пространством, где защита детей от информационных угроз должна обеспечиваться последовательно и системно, однако реальное состояние дел во многих российских образовательных учреждениях указывает на значительные пробелы как в правовом регулировании этой сферы, так и в организационных механизмах её реализации.*

Ключевые слова: *правовая квалификация, киберугрозы, Правовое регулирование, информационная безопасность.*

AKAPYEV Viktor Lvovich,
Candidate of Pedagogical Sciences, Docent of the Department of Information and Computer Technologies in the Activities of Law Enforcement Agencies Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin

KOVALEVA Ekaterina Gennadievna,
Candidate of Technical Sciences, Associate Professor of the Department of Information and Computer Technologies in the Activities of Law Enforcement Agencies Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin

BORISENKO Alexander Vasilyevich,
Candidate of Physico-mathematical Sciences, Senior lecturer of the Department of Information and Computer Technologies in the Activities of Law Enforcement Agencies Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin

NOVIKOVA Ekaterina Anatolyevna,
Candidate of Law, Associate Professor, Head of the Department of Information and Computer Technologies in the Activities of Law Enforcement Agencies Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I.D. Putilin

LEGAL METHODS OF ENSURING INFORMATION SECURITY FOR SCHOOLCHILDREN

Annotation. *Modern society is undergoing a profound transformation, which is based on the rapid spread of digital technologies that cover almost all areas of human life, including education, leisure, professional activities, and everyday communication. School-age children are immersed in the digital environment much earlier than they have the opportunity to develop stable ideas about safe behavior in it, and this is what makes the issue of their information security one of the most pressing social problems of our time. First of all, it is necessary to note the steady increase in the number of cyber threats faced by underage Internet users. At the same time, children's ability to recognize such threats on their own is significantly limited due to their lack of life experience and low level of digital literacy. As the primary institution for socialization, schools should provide consistent and systematic protection against information threats, but the current state of affairs in many Russian educational institutions reveals significant gaps in both legal regulation and organizational mechanisms for implementing such protection.*

Key words: *legal qualification, cyber threats, legal regulation, and information security.*

Правовое регулирование информационной безопасности несовершеннолетних в Российской Федерации в последние годы заметно развивалось: были приняты важные законодательные акты, направленные на защиту детей от вредоносного контента и ограничение их доступа к информации, причиняющей ущерб нравственному и психическому развитию [1]. Вместе с тем правоприменительная практика обнаруживает очевидную недостаточность существующих механизмов, поскольку нормативные предписания нередко остаются декларативными при отсутствии чётко выстроенной системы их исполнения на уровне конкретных образовательных организаций. Это противоречие между формально закреплёнными правовыми гарантиями и реальным уровнем защищённости школьников в цифровой среде составляет один из ключевых исследовательских вопросов настоящей работы.

Современное общество устроено таким образом, что информация давно превратилась в один из ключевых ресурсов, от состояния кото-

рого зависит не только работа государственных структур и коммерческих организаций, но и повседневная жизнь каждого человека, включая детей школьного возраста. Информация сопровождает человека на каждом шагу: в процессе обучения, общения, досуга и самовыражения, а её доступность через цифровые устройства и интернет сделала вопросы защиты этой информации крайне актуальными для всех возрастных групп населения. Именно поэтому понятие информационной безопасности сегодня рассматривается не только как технический вопрос, но и как правовая, социальная и педагогическая проблема, требующая комплексного подхода со стороны государства, образовательных организаций и семьи.

Информационная безопасность в самом широком смысле представляет собой состояние защищённости информационной среды, при котором обеспечивается сохранность, целостность и доступность информации, а также защита интересов людей, организаций и государства от негативного информационного воздействия. Это понятие охватывает сразу несколько уровней: технический, на котором речь идёт о защите данных и программного обеспечения; правовой, предполагающий наличие законодательных норм, регулирующих информационные отношения; и социально-психологический, связанный с влиянием информационной среды на сознание и поведение человека. Для понимания информационной безопасности школьников особенно важен именно третий уровень, поскольку дети и подростки наиболее восприимчивы к воздействию контента и способам его подачи в цифровом пространстве.

В российском законодательстве понятие информационной безопасности закреплено в Доктрине информационной безопасности Российской Федерации, утверждённой Указом Президента от 5.12.2016 года № 646, где под ней понимается состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, обеспечивающее реализацию конституционных прав и свобод, достойное качество и уровень жизни граждан, суверенитет и устойчивое развитие страны. Этот документ закладывает концептуальные основы государственной политики в данной сфере и определяет ключевые направления деятельности органов власти по обеспечению защиты информационного пространства. Помимо этого, правовое регулирование информационной безопасности осуществляется через Федеральный закон об информации, информационных технологиях и о защите информации, Федеральный закон о защите детей от информации, причиняющей вред их здоровью и развитию, а также ряд подзаконных актов и ведомственных документов [2].

Угрозы информационной безопасности принято делить на несколько групп в зависимости от их природы и источника. Внешние угрозы исходят из цифрового пространства и включают распространение вредоносного программного обеспечения, кибермошенничество, незаконный сбор персональных данных, а также распространение контента, наносящего психологический вред пользователям [3]. Внутренние угрозы связаны с действиями самих пользователей, в том числе с неосторожным обращением с личными данными, неосознанным распространением опасной информации и отсутствием цифровой грамотности. Применительно к школьникам обе группы угроз особенно значимы, поскольку дети зачастую не обладают достаточным уровнем критического мышления и опыта, чтобы самостоятельно распознать ту или иную угрозу и правильно на неё отреагировать.

Отдельного внимания заслуживает понятие информационной безопасности личности, под которой понимается защита психологического состояния, ценностных ориентиров, мировоззрения и поведения человека от деструктивного информационного воздействия. Для несовершеннолетних этот аспект имеет принципиальное значение, поскольку их психика находится в стадии формирования, а потому воздействие агрессивного, манипулятивного или пропагандистского контента может нанести серьёзный и долгосрочный вред их развитию [4]. Исследования в области детской и подростковой психологии подтверждают, что регулярный контакт с негативным цифровым контентом способен формировать искажённую картину мира, провоцировать тревожность, агрессию и снижение социальной адаптации у детей школьного возраста.

Система обеспечения информационной безопасности строится на нескольких взаимосвязанных принципах, без соблюдения которых достижение реальной защищённости невозможно. Принцип законности предполагает, что все меры по защите информации и ограничению доступа к вредоносному контенту должны опираться на действующие нормы права и не нарушать конституционных прав граждан. Принцип комплексности означает, что защита должна осуществляться одновременно на нескольких уровнях и включать технические, правовые, организационные и просветительские меры. Принцип непрерывности требует постоянного мониторинга информационной среды и своевременного реагирования на возникающие угрозы, а не разовых точечных вмешательств. Наконец, принцип соразмерности предполагает, что применяемые ограничения и защитные меры должны быть адекватны реальному уровню угрозы и не должны создавать

избыточных препятствий для законного использования информации [5].

Таким образом, информационная безопасность представляет собой многоуровневое явление, охватывающее технические, правовые и социальные аспекты защиты человека и общества от негативных информационных воздействий. В контексте обеспечения безопасности школьников она приобретает особую значимость, поскольку затрагивает не только вопросы защиты данных, но и охрану психического здоровья, нормального интеллектуального и нравственного развития детей в условиях цифровой среды, которая становится для них всё более привычным пространством жизни и общения.

Следовательно, научный и практический интерес представляет направление информационной безопасности в образовательной среде, которое охватывает несколько самостоятельных, но взаимосвязанных траекторий, каждая из которых имеет собственную природу, собственные инструменты реализации и собственные проблемные точки, однако все они в конечном счёте работают на одну цель: обеспечить детям и педагогам безопасное, контролируемое и педагогически обоснованное пространство для работы с информацией. Рассмотрение каждого вида в отдельности позволяет лучше понять, каким образом они встраиваются в общую логику защиты образовательного процесса.

Первым и наиболее очевидным видом является техническая информационная безопасность, которая связана с защитой цифровой инфраструктуры школы: компьютерного оборудования, локальных сетей, серверов, учётных записей, баз данных с персональными данными учеников и педагогов. В большинстве российских школ этот вид безопасности реализуется через установку антивирусного программного обеспечения, настройку межсетевых экранов, разграничение прав доступа к файлам и папкам, а также через использование систем контентной фильтрации, блокирующих доступ к нежелательным интернет-ресурсам [1]. Проблема состоит в том, что уровень технической защиты в разных школах существенно различается: в крупных городских учреждениях, как правило, имеется системный администратор, который следит за состоянием инфраструктуры, тогда как в небольших сельских школах обслуживание техники нередко возложено на учителя информатики, не имеющего специальной квалификации в области информационной безопасности. Это порождает структурное неравенство в уровне защищённости, и для его преодоления целесообразно предусмотреть централизованную техническую поддержку со стороны муниципальных органов управления образованием, которые могли бы обеспечивать дистанционное администрирование, плановые проверки состояния сетевой инфраструктуры и своевременное обновление программного обеспечения на всех подведомственных объектах. Кроме того, техническая безопасность требует регулярного резервного копирования данных, поскольку потеря электронного журнала или архива личных дел учащихся способна нанести серьёзный ущерб работе учреждения.

Вторым важным видом является правовая информационная безопасность, которая обеспечивает соответствие деятельности школы действующему законодательству в информационной сфере. Здесь речь идёт прежде всего о выполнении требований Федерального закона № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона № 152-ФЗ «О персональных данных», Федерального закона № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», а также ряда подзаконных актов, регулирующих порядок хранения и обработки сведений об учащихся. На практике правовая безопасность реализуется через разработку и утверждение локальных нормативных актов школы: политики обработки персональных данных, положения об использовании информационных ресурсов, правил работы с электронными системами. Слабым местом этого направления является то, что многие школы формально выполняют требования закона, размещая на сайте соответствующие документы, но не обеспечивают их реального соблюдения в повседневной практике. Например, согласия родителей на обработку персональных данных собираются, но затем данные передаются сторонним сервисам без должного контроля. Для совершенствования правовой составляющей безопасности рекомендуется проводить ежегодный внутренний аудит соответствия документации актуальным требованиям законодательства, поскольку нормативная база в этой сфере регулярно обновляется и локальные акты, разработанные несколько лет назад, могут уже не отвечать действующим нормам.

Третьим видом выступает организационная информационная безопасность, которая касается выстраивания внутри школы чётких процедур, распределения обязанностей и создания системы контроля за информационной средой. Организационные меры включают назначение ответственного за информационную безопасность, разработку инструкций для педагогов и технического персонала, установление порядка реагирования на инциденты, а также проведение инструктажей и внутреннего обучения. В образовательной организации организационная безопасность нередко

недооценивается, поскольку руководство склонно считать, что технические меры сами по себе достаточны. Между тем именно организационная составляющая создаёт условия, при которых технические средства работают правильно: если педагог не знает, что нельзя открывать подозрительные вложения в электронной почте, никакой антивирус не спасёт от заражения школьного сервера. Совершенствование этого вида безопасности предполагает внедрение практики регулярных учебных тренингов для сотрудников по основам цифровой гигиены, а также создание понятного и доступного регламента действий в случае выявления инцидента, например, при утечке персональных данных или несанкционированном доступе к школьным ресурсам.

Четвёртым видом является психологическая информационная безопасность, направленная на защиту психического состояния школьников от деструктивного воздействия информационной среды. Этот вид безопасности связан с рисками, которые несут в себе кибербуллинг, вовлечение детей в деструктивные сообщества в социальных сетях, распространение контента, пропагандирующего суицид, насилие, экстремизм или расстройства пищевого поведения. В отличие от технических угроз, психологические угрозы значительно труднее поддаются обнаружению и нейтрализации, поскольку ребёнок нередко скрывает от взрослых факт своего участия в опасных коммуникациях. Реализация этого вида безопасности в образовательной среде осуществляется преимущественно через работу школьного психолога, классных руководителей и родителей, а также через включение в учебный план занятий по медиаграмотности и безопасному поведению в сети. Для повышения эффективности психологической защиты целесообразно выстраивать в школе систему раннего выявления признаков вовлечённости детей в деструктивные группы, опираясь не только на наблюдение педагогов, но и на специализированные методики работы школьного психолога, которые позволяют своевременно замечать изменения в поведении учащихся.

Пятым видом является содержательная, или педагогическая, информационная безопасность, которая касается качества и характера информации, используемой в учебном процессе. Этот вид безопасности предполагает, что информация, с которой работают школьники в рамках образовательной деятельности, соответствует их возрасту, педагогически обоснована и не наносит вреда их развитию. Реализуется это направление через отбор учебных материалов, использование проверенных образовательных платформ, контроль за содержанием мультимедийных ресурсов, применяемых на уроках, а также через формирование у учащихся навыков критического анализа информации. Проблема состоит в том, что стремительное развитие цифровых технологий опережает возможности педагогического сообщества по оценке новых инструментов, поэтому учителя нередко используют на уроках приложения и сервисы, которые не проходили никакой педагогической экспертизы. В целях совершенствования этого направления представляется полезным создание на уровне региона или федерации реестра рекомендованных цифровых образовательных ресурсов с указанием возрастных ограничений и методических рекомендаций по их применению, что позволило бы педагогам ориентироваться в многообразии доступных инструментов и осознанно выбирать безопасные и эффективные из них.

Таким образом, информационная безопасность в образовательной среде представляет собой многокомпонентную систему, в которой технические, правовые, организационные, психологические и содержательные элементы взаимодействуют между собой и взаимно дополняют друг друга. Отсутствие хотя бы одного из этих компонентов существенно снижает уровень защищённости школьников, поскольку угрозы в информационной сфере носят комплексный характер и не могут быть нейтрализованы усилиями только одного направления. Именно поэтому организационно-правовые методы должны рассматриваться не в изоляции, а в системной взаимосвязи с иными видами мер, направленных на обеспечение безопасности детей в цифровой среде, что позволяет выстроить по-настоящему устойчивую и работоспособную модель защиты.

Система управления информационной безопасностью в образовательной организации представляет собой совокупность взаимосвязанных элементов, которые в совокупности обеспечивают защиту обучающихся, педагогов и административного персонала от угроз в цифровом пространстве, а также гарантируют сохранность персональных данных, образовательного контента и технической инфраструктуры учреждения. Говоря об этой системе, важно понимать, что она не сводится исключительно к установке антивирусного программного обеспечения или настройке сетевых фильтров, а охватывает значительно более широкий спектр управленческих, педагогических, правовых и технических решений, которые должны функционировать согласованно и на постоянной основе.

Фундаментом всей системы управления информационной безопасностью в образовательном учреждении служит нормативно-правовая база, которая задаёт рамки допустимого и обязательного поведения всех участников образо-

вательного процесса в информационной среде. На уровне школы это выражается в разработке и утверждении внутренних локальных актов, в частности положений об использовании информационных ресурсов, политик доступа к сети интернет, регламентов обработки персональных данных учащихся и сотрудников, а также должностных инструкций для лиц, ответственных за информационную безопасность [5]. Однако на практике нередко встречается ситуация, когда подобные документы формально существуют, но фактически не исполняются, поскольку их содержание устарело, не учитывает реальных технологических условий или просто незнакомо педагогическому коллективу. Для исправления этого положения целесообразно проводить ежегодный аудит внутренней нормативной базы с привлечением специалиста в области информационных технологий и юриста, что позволит своевременно актуализировать документы и привести их в соответствие с действующим законодательством и реальными потребностями школы.

Следующим ключевым элементом системы управления выступает организационная структура, то есть распределение ответственности за информационную безопасность между конкретными людьми внутри учреждения. В большинстве российских школ эта функция возложена на системного администратора, который одновременно занимается технической поддержкой оборудования, настройкой программного обеспечения и обеспечением сетевой безопасности, что создаёт очевидную перегрузку и снижает качество каждого из направлений работы. Более рациональным подходом было бы выделение отдельной должности или хотя бы отдельного функционала для специалиста по информационной безопасности, в обязанности которого входили бы мониторинг угроз, обучение персонала, взаимодействие с контролирующими органами и разработка защитных мер. Помимо этого, в систему управления целесообразно включать заместителя директора по учебно-воспитательной работе, классных руководителей и школьного психолога, поскольку многие угрозы информационной безопасности для детей носят не технический, а психологический и поведенческий характер, и именно педагоги первыми способны заметить признаки вовлечения ребёнка в опасные онлайн-сообщества или факты кибербуллинга.

Техническое обеспечение системы управления информационной безопасностью охватывает весь спектр программных и аппаратных средств, с помощью которых школа защищает свою инфраструктуру и контролирует информационную среду. К таким средствам относятся системы контентной фильтрации, ограничивающие доступ учащихся к нежелательным интернет-ресурсам, межсетевые экраны, предотвращающие несанкционированное проникновение в школьную сеть, системы резервного копирования данных, защищающие от потери информации вследствие технических сбоев или вредоносных атак, а также средства антивирусной защиты на всех рабочих станциях и серверах учреждения. Вместе с тем одной лишь установки этих инструментов недостаточно, поскольку технические средства требуют регулярного обновления, профессиональной настройки и мониторинга их работоспособности. Для повышения эффективности технической составляющей системы управления представляется целесообразным внедрение централизованной системы мониторинга сети, которая позволяла бы в режиме реального времени отслеживать подозрительную активность и оперативно реагировать на инциденты, не дожидаясь их перехода в серьёзную проблему [1].

Не менее важным направлением является работа с персоналом, которая в контексте информационной безопасности предполагает систематическое повышение цифровой грамотности педагогов и технических сотрудников. Значительная часть инцидентов в области информационной безопасности происходит не вследствие изощрённых хакерских атак, а по причине банальной неосторожности пользователей, открывающих фишинговые письма, использующих слабые пароли или подключающих непроверенные устройства к школьной сети. Регулярные тренинги, практические занятия по распознаванию угроз и чёткие инструкции по поведению при возникновении инцидента способны существенно снизить вероятность подобных ошибок. В качестве меры по совершенствованию этого направления можно предложить введение обязательного ежегодного инструктажа по информационной безопасности для всех сотрудников школы с последующей проверкой усвоенных знаний, что позволит не только повысить осведомлённость персонала, но и зафиксировать факт прохождения обучения в документальном порядке.

Отдельного внимания заслуживает работа с учащимися, которая представляет собой один из наиболее сложных и одновременно наиболее значимых элементов системы управления информационной безопасностью в школе. Дети и подростки являются наиболее уязвимой категорией пользователей цифровой среды, поскольку в силу возрастных особенностей они склонны к доверчивости, импульсивному поведению в сети и недооценке реальных рисков онлайн-общения. Формирование у школьников навыков безопасного поведения в интернете должно осуществляться не в форме разовых лекций или запретительных

мер, а в рамках системной образовательной работы, встроенной в учебный процесс и внеурочную деятельность. Для этого целесообразно разработать специализированный курс или модуль по цифровой безопасности, адаптированный для разных возрастных групп, поскольку угрозы и модели поведения младших школьников существенно отличаются от тех, с которыми сталкиваются старшеклассники, и единый подход здесь явно недостаточен [6].

Важнейшей частью системы управления информационной безопасностью является взаимодействие школы с родителями, которые в большинстве случаев не имеют возможности напрямую контролировать поведение детей в интернете и при этом нередко сами обладают недостаточным уровнем цифровой грамотности. Родительские собрания, посвящённые вопросам безопасности детей в сети, информационные буклеты и рекомендации по использованию родительского контроля позволяют вовлечь семью в процесс защиты ребёнка и создать согласованную среду, в которой правила безопасного поведения действуют не только в школе, но и дома. В качестве перспективного направления совершенствования данного элемента системы можно предложить создание закрытого информационного портала или раздела на школьном сайте, где родители могли бы получать актуальные сведения об угрозах, рекомендации специалистов и инструменты для самостоятельного обучения цифровой безопасности.

Управление инцидентами информационной безопасности составляет ещё одну важную подсистему, которая нередко остаётся неразвитой в большинстве школ. Под управлением инцидентами понимается совокупность процедур, определяющих порядок выявления, регистрации, расследования и устранения последствий нарушений в области информационной безопасности, будь то утечка персональных данных, заражение оборудования вредоносным программным обеспечением, несанкционированный доступ к учебным материалам или факт кибербуллинга. Отсутствие чётко описанного алгоритма действий в таких ситуациях приводит к хаотичному реагированию, затягиванию сроков устранения угрозы и невозможности объективно оценить масштаб ущерба. Совершенствование этого направления предполагает разработку и утверждение внутреннего регламента реагирования на инциденты, в котором будут закреплены конкретные роли, сроки и последовательность действий каждого ответственного лица, что позволит действовать организованно даже в условиях стресса и неопределённости.

Наконец, система управления информационной безопасностью не может функционировать эффективно без регулярной оценки её результативности, которая осуществляется посредством внутренних и внешних проверок, анализа статистики инцидентов, мониторинга технического состояния инфраструктуры и изучения уровня осведомлённости участников образовательного процесса. Именно контрольная функция замыкает управленческий цикл и позволяет выявлять слабые места, вносить необходимые коррективы и поддерживать систему в актуальном состоянии.

Для повышения качества этой работы представляется обоснованным привлечение внешних экспертов или специализированных организаций для проведения независимого аудита информационной безопасности школы не реже одного раза в два года, а также внедрение практики самооценки с использованием стандартизированных методик, что создаст условия для постоянного совершенствования всей системы в целом.

Таким образом, процесс обеспечения информационной безопасности в образовательной организации представляет собой многоуровневое явление, охватывающее технические, правовые и социальные аспекты защиты человека и общества от негативных информационных воздействий. В контексте обеспечения безопасности школьников она приобретает особую значимость, поскольку затрагивает не только вопросы защиты данных, но и охрану психического здоровья, нормального интеллектуального и нравственного развития детей в условиях цифровой среды, которая становится для них всё более привычным пространством жизни и общения.

Информационная безопасность в образовательной среде представляет собой многокомпонентную систему, в которой технические, правовые, организационные, психологические и содержательные элементы взаимодействуют между собой и взаимно дополняют друг друга. Отсутствие хотя бы одного из этих компонентов существенно снижает уровень защищённости школьников, поскольку угрозы в информационной сфере носят комплексный характер и не могут быть нейтрализованы усилиями только одного направления. Именно поэтому организационно-правовые методы, которым посвящена настоящая работа, должны рассматриваться не в изоляции, а в системной взаимосвязи с иными видами мер, направленных на обеспечение безопасности детей в цифровой среде, что позволяет выстроить по-настоящему устойчивую и работоспособную модель защиты.

Система управления информационной безопасностью не может функционировать эффективно без регулярной оценки её результативности, которая осуществляется посредством внутренних и внешних проверок, анализа статистики

инцидентов, мониторинга технического состояния инфраструктуры и изучения уровня осведомлённости участников образовательного процесса. Именно контрольная функция замыкает управленческий цикл и позволяет выявлять слабые места, вносить необходимые коррективы и поддерживать систему в актуальном состоянии. Для повышения качества этой работы представляется обоснованным привлечение внешних экспертов или специализированных организаций для проведения независимого аудита информационной безопасности школы не реже одного раза в два года, а также внедрение практики самооценки с использованием стандартизированных методик, что создаст условия для постоянного совершенствования всей системы в целом.

Список литературы:

[1] Барков, А.В., Киселев, А.С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право. 2022. № 4. С. 20 – 27.

[2] Дубень А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению // Международное право и международные организации. 2022. № 1. С. 24 – 30.

[3] Комплексные решения обеспечения информационной безопасности персональных данных: Учебник / В.Л. Акапьев, А.В. Борисенко, Е.Г. Ковалева, Е.А. Новикова. – Санкт-Петербург: Наукоемкие технологии, 2026. – 110 с.

[4] Дугенец А.С., Павлова Л.В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. 2023. № 5. С. 22 – 25.

[5] Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. М.: Юрайт. 2023. 343 с.

[6] Зенков А.В. Основы информационной безопасности. Учебное пособие. М.: Инфра-Инженерия. 2022. 104 с.

References:

[1] Barkov, A.V., Kiselev, A.S. On the legal security of the information and telecommunication infrastructure of banks and government agencies // Banking Law. 2022. № 4. S. 20-27.

[2] Duben A.K. International cooperation in the field of information security: a general description and the Russian approach to study // International law and international organizations. 2022. № 1. S. 24-30.

[3] Comprehensive solutions for ensuring information security of personal data: Textbook/ V.L. Akapiev, A.V. Borisenko, E.G. Kovaleva, E.A. Novikova. - St. Petersburg: Science-intensive technologies, 2026. - 110 s.

[4] Dugenets A.S., Pavlova L.V. State regulation of ensuring the information security of minors as a component of the national security of Russia // Administrative law and process. 2023. № 5. S. 22-25.

[5] Kazarin O.V., Shubinsky I.B. Fundamentals of information security: reliability and security of software. M.: Yurayt. 2023. 343 pp.

[6] A.V. Zenkov. Fundamentals of Information Security. Tutorial. M.: Infra-Engineering. 2022. 104 p.