. ОСНОВЫ И СПЕЦИФИКА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ ИНТЕРНАТНОГО ТИПА

М.А. Лем[1], *магистрант*
Научный руководитель: *А.В. Минаев, канд. юрид. наук, доцент[1], профессор[2]*
[1]Калининградский институт управления
[2]Академия военных наук
[1,2](Россия, г. Калининград)

DOI:10.24412/2500-1000-2026-6-2-297-304

Аннотация. *В статье рассматривается эволюция доктринального закрепления понятия «информационная безопасность» в Российской Федерации и её влияние на систему образования. Особое внимание уделено специфике учреждений интернатного типа для лиц с ограниченными возможностями здоровья, которые одновременно выполняют функции профессиональной образовательной организации и поставщика социальных услуг. На основе анализа нормативно-правовой базы и научной литературы выявлены и систематизированы угрозы информационной безопасности, характерные для данного контингента обучающихся, с учётом их когнитивных и психоэмоциональных особенностей. В статье предлагается классификация угроз по нозологическим группам и трёхуровневая модель их эскалации. Сформулирован вывод, что выявленные теоретические проблемы требуют проведения комплексного эмпирического анализа системы информационной безопасности конкретного учреждения интернатного типа.*

Ключевые слова: *информационная безопасность; Доктрина информационной безопасности; образовательное учреждение интернатного типа; обучающиеся с ограниченными возможностями здоровья; ментальные нарушения; угрозы информационной безопасности.*

Современный этап развития информационного общества характеризуется беспрецедентным ростом значимости информационной сферы, которая оказывает системообразующее влияние на все стороны государственной и общественной жизни. В этих условиях обеспечение информационной безопасности становится одним из приоритетных направлений государственной политики, что нашло отражение в Доктрине информационной безопасности Российской Федерации, утверждённой в 2016 году [1]. Однако стремительная эволюция киберугроз, цифровизация образования и появление новых уязвимостей требуют постоянной актуализации доктринальных установок. Не случайно Совет Безопасности РФ с сентября 2025 года ведёт разработку новой редакции Доктрины, в которой предполагается закрепить принцип неразрывности защиты информации на всех этапах создания и эксплуатации цифровых систем [15].

Особую остроту вопросы информационной безопасности приобретают для образовательных учреждений интернатного типа, находящихся в ведении органов социальной защиты. Их контингент (дети-инвалиды и лица с ограниченными возможностями здоровья, в том числе с ментальными нарушениями), обладает повышенной уязвимостью перед информационно-психологическими угрозами. Круглосуточное пребывание обучающихся на территории учреждения и двойное подчинение (одновременно Минпросвещения России и региональным органам соцзащиты) формируют уникальную, трудно воспроизводимую в иных организациях конфигурацию рисков. Однако, несмотря на очевидную актуальность данной проблемы, комплексных исследований, посвящённых анализу системы информационной безопасности именно в учреждениях интернатного типа для лиц с ОВЗ, до настоящего времени не проводилось. На восполнение этого теоретического пробела и направлена настоящая работа. Методологическую основу исследования составили системный и междисциплинарный подходы, позволившие рассмотреть информационную безопасность образовательного учреждения интернатного типа как совокупность правовых, организационных, технических и психолого-педагогических элементов. В процессе исследования использовались методы анализа и синтеза научной

литературы, сравнительно-правовой анализ нормативных правовых актов Российской Федерации в сфере информационной безопасности, образования и социальной защиты населения, классификация систематизации угроз, характерных для обучающихся лиц с ограниченными возможностями здоровья. Теоретическую основу исследования были использованы труды Российских авторов в области информационной безопасности, специальной психологии и виктимологии, педагогики.

Эволюция понимания «информационной безопасности» в Российской Федерации, тесно связано с развитием технологий в области информации, а также стремительно меняющейся геополитикой. Первоисточником послужил Закон РФ «О государственной тайне» 1993 года, в его основе были заложены основы защиты секретной информации, однако само понятие «информационная безопасность» долгое время оставалось размытым и не имело единого доктринального закрепления.

Ключевую роль в систематизации государственной политики в данной сфере сыграла Доктрина информационной безопасности Российской Федерации, утверждённая Президентом РФ 9 сентября 2000 года. Этот документ впервые на официальном уровне определил информационную безопасность как состояние защищённости национальных интересов в информационной сфере. В научной литературе отмечается, что раскрытие категории правовой защиты информации в рамках Доктрины 2000 года можно охарактеризовать как достаточное и полноценное. Документ зафиксировал четыре основные составляющие национальных интересов в информационной сфере и предложил комплекс правовых, организационно-технических и экономических методов их обеспечения [7].

За шестнадцать лет действия Доктрины 2000 года информационная сфера претерпела кардинальные изменения. Широкое распространение сети Интернет, появление социальных сетей, рост киберпреступности и усиление информационного противоборства на международной арене потребовали актуализации доктринальных установок, в следствии чего в 2016 году была утверждена новая Доктрина информационной безопасности Российской Федерации. Авторы научных исследований отмечают, что в современных геополитических реалиях появляется потребность в адаптивных подходах к обеспечению безопасности [8].

В Доктрине 2016 года было расширено понятие информационной безопасности: «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [1]. В данном определении можно видеть, что разработчики фактически интегрировали в понятие информационной безопасности весь спектр целей национальной безопасности, что, с одной стороны, подчёркивает системообразующую роль информационной сферы, а с другой – порождает определённые терминологические сложности.

Несмотря на очевидную актуальность принятия Доктрины 2016 года, в научном сообществе она подверглась достаточно обстоятельной критике. Ряд исследователей указывают, что по структуре, полноте правового регулирования и другим важным характеристикам Доктрина 2016 года, по своему содержанию, не является адаптированным под современные вызовы правовым актом, в сравнении с предыдущей Доктриной [8]. Отмечается аморфность определения информационной сферы, наличие повторов и дублирующих друг друга положений, а также отсутствие чёткого разграничения задач государственных органов.

Ещё один важный аспект критики связан со смещением доктринальных приоритетов. В ряде научных исследований было отмечено, что если ранее важность проработки правовых аспектов информационной безопасности не вызывала сомнения, то теперь видно явное стремление государства в рамках международных отношений, вывести всю информационную сферу на качественно новый уровень, где информационные технологии и их совершенствование выступают Доминирующими категориями [7]. В Доктрине 2016 года правовые методы лишь упоминаются в общем перечне средств наряду с организационными и техническими, что создаёт предпосылки для недооценки правового регулирования как

важнейшего инструмента защиты информационной сферы.

Наиболее острая критика действующей Доктрины содержится в работе, опубликованной в 2024 году [9]. Автор обращает внимание на то, что Доктрина 2016 года уже действует длительное время без изменений, что в современных геополитических условиях не может быть ничем оправданным. За это время была принята новая Стратегия национальной безопасности, началась специальная военная операция (СВО), многократно возросло информационное давление на Россию, однако документ стратегического планирования ни разу не корректировался, в следствие чего, Доктрина 2016 года по содержанию ссылается Стратегию национальной безопасности от 31 декабря 2015 года [9]. Кроме того, в Доктрине существует разность терминологии: понятийный ряд Доктрины 2016 года не соответствует легальным определениям, содержащимся в более общих документах стратегического планирования, а отдельные формулировки национальных интересов носят аморфный характер, обусловливая отсутствие правовых последствий его обеспечения, реализации и защиты [9].

Вместе с тем Доктрина 2016 года содержит ряд принципиально важных целевых установок, непосредственно затрагивающих систему образования. Так, в качестве одной из стратегических целей обеспечения информационной безопасности в области науки, технологий и образования названо «развитие кадрового потенциала в области обеспечения информационной безопасности», а также закреплена необходимость «формирования у граждан культуры личной информационной безопасности» [1, п. 26]. Именно на образовательные организации, включая учреждения среднего профессионального образования, возлагается решение этих задач государственной важности.

Следовательно, эволюция доктринального закрепления понятия «информационная безопасность» демонстрирует, с одной стороны, возрастающее внимание государства к информационной сфере как к системообразующему фактору национальной безопасности, а с другой – наличие неразрешённых проблем правового и организационного характера. Недостаточная проработанность дефиниций, отставание доктринальных установок от динамично меняющейся реальности и ослабление внимания к правовым механизмам защиты информации создают ситуацию, при которой значительная часть ответственности за практическое обеспечение информационной безопасности переносится с федерального уровня на уровень конкретных организаций. При этом образовательные учреждения оказываются в двойственном положении: они не только обязаны защищать собственные информационные системы и персональные данные, но и призваны реализовывать доктринальные цели по формированию кадров и воспитанию культуры информационной безопасности, что требует от них активной адаптации общих стратегических ориентиров к своей специфике.

Образовательное учреждение как объект информационной защиты: общая характеристика угроз. Современное образовательное учреждение представляет собой сложный объект информационной защиты, что обусловлено его двойственной природой. С одной стороны, оно выступает активным участником информационного обмена и оператором значительных массивов данных, с другой – является средой формирования личности несовершеннолетних и лиц с ограниченными возможностями здоровья. В соответствии с Доктриной информационной безопасности Российской Федерации и положениями Федерального закона «Об информации, информационных технологиях и о защите информации» защита информации в образовательной организации должна обеспечиваться на всех этапах её создания, передачи, хранения и уничтожения. При этом образовательные учреждения, включая организации интернатного типа, дополнительно подпадают под действие Федерального закона «О персональных данных» и Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», что формирует многоконтурную систему нормативных требований к защите информационной среды [1-4].

Классификация угроз информационной безопасности образовательного учреждения традиционно осуществляется по нескольким основаниям. По источнику возникновения угрозы подразделяются на внешние и внутренние. Внешние исходят от субъектов, не относящиеся к образовательной организации: кибератаки, DDoS-атаки на информационные системы, на сайты и сервисы дистанционного обучения, распространение вредоносного

программного обеспечения, фишинговые рассылки, попытки неправомерного доступа к базам персональных данных извне. Исследователи отмечают, что современное пространство киберугроз постоянно совершенствуется, рождая новые вызовы как для различного рода организаций, так и для пользователей по всему миру, где злоумышленники активно стараются совершенствовать свои методы атак, что в свою очередь требует непрерывной работы по обновлению стратегий обеспечения безопасности [10]. Внутренние угрозы связаны с действиями или бездействием сотрудников и обучающихся: ошибки при обработке конфиденциальной информации, непреднамеренное заражение системы вредоносными программами, нарушение установленных регламентов работы, умышленные нарушения со стороны нелояльных сотрудников, а также низкий уровень культуры информационной безопасности. Как справедливо отмечается в научной литературе, человеческий фактор остаётся одним из наиболее уязвимых звеньев любой системы защиты, а концепция «человек – слабое звено» требует пристального внимания при выстраивании организационных мер [11].

По объекту воздействия угрозы следует рассматривать применительно к трём основным группам активов образовательной организации: информационной инфраструктуре, данным и личности участников образовательного процесса. Первая группа – угрозы конфиденциальности персональных данных – имеет для образовательных учреждений приоритетное значение. Согласно Федеральному закону «О персональных данных», образовательная организация признаётся оператором, обрабатывающим персональные данные обучающихся, их законных представителей и работников [3]. В учреждениях интернатного типа дополнительно обрабатываются специальные категории персональных данных, касающиеся состояния здоровья и инвалидности, что существенно повышает требуемый уровень защищённости информационных систем. Вторая группа – угрозы целостности и доступности информационных систем – охватывает риски, способные парализовать учебный процесс: DDoS-атаки, вредоносное программное обеспечение, в том числе программы-шифровальщики, а также физические сбои серверного и сетевого оборудования. Третья группа – угрозы информационно-психологического воздействия на обучающихся – заслуживает отдельного внимания в силу возрастных и психологических особенностей контингента. К числу наиболее опасных явлений в образовательной среде относятся кибербуллинг, вовлечение в экстремистские и террористические сообщества через социальные сети и мессенджеры, а также целенаправленные манипуляции, эксплуатирующие доверчивость и недостаточную критичность мышления обучающихся.

Специфика угроз информационной безопасности для контингента с ОВЗ. Обучающиеся с ограниченными возможностями здоровья входят в особую категорию участников образовательного процесса, чья уязвимость многократно превышает аналогичные показатели для нормативно развивающихся сверстников перед угрозами информационной безопасности. Данное обстоятельство обусловлено комплексом факторов – когнитивных, эмоционально-волевых, коммуникативных и социальных, – которые в своей совокупности формируют специфический профиль риска. Учёт этой специфики является обязательным условием построения эффективной системы информационной защиты в образовательных организациях, реализующих адаптированные образовательные программы, в том числе в учреждениях интернатного типа.

Современные исследования фиксируют, что дети с ОВЗ впервые знакомятся с информационными устройствами в возрасте 5-7 лет, около 40% из них посещают интернет-пространство ежедневно, а свыше половины их родителей в качестве основных средств обеспечения безопасности в цифровой среде указывают установку защитных программ и проведение профилактических бесед [12]. При этом сами родители не всегда способны адекватно оценить уровень цифровых угроз, с которыми сталкивается ребёнок с нарушениями развития, что создаёт дополнительный разрыв между реальной и воспринимаемой защищённостью [12].

Наибольшую группу риска составляют обучающиеся с ментальными нарушениями (умственной отсталостью, задержкой психического развития, расстройствами аутистического спектра). Исследования показывают, что их уязвимость перед онлайн-угрозами

обусловлена специфическими характеристиками: ограниченными когнитивными способностями (трудности с критическим и абстрактным мышлением, неспособность к полноценному анализу ситуации и прогнозированию последствий своих действий); повышенной доверчивостью к незнакомцам и склонностью воспринимать любую информацию как достоверную; трудностями с распознаванием социальных сигналов, в том числе агрессивного или манипулятивного поведения в цифровой среде; ограниченной способностью к саморегуляции, ведущей к риску формирования интернет-аддикции; а также завышенной самооценкой и нарушением критичности, препятствующими адекватной оценке собственной уязвимости [13]. Указанные особенности создают благоприятную почву для виктимизации обучающихся данной категории в цифровом пространстве. Для более наглядной дифференциации информационных угроз целесообразно представить их зависимость от нозологической принадлежности обучающихся с ОВЗ (табл.).

Таблица. Дифференциации информационных угроз в зависимости от нозологической принадлежности обучающихся с ОВЗ

Нозологическая группа	Основные факторы уязвимости	Приоритетные угрозы
Обучающиеся с интеллектуальными нарушениями (умственная отсталость)	Низкая критичность мышления, высокая внушаемость, трудности прогнозирования последствий	Онлайн-мошенничество, груминг, кибербуллинг, кража персональных данных
Обучающиеся с задержкой психического развития	Незрелость эмоционально-волевой сферы, повышенная зависимость от мнения группы	Кибербуллинг, вовлечение в деструктивные интернет-сообщества, интернет-аддикция
Обучающиеся с расстройствами аутистического спектра	Трудности интерпретации социальных сигналов и распознавания манипуляций	Груминг, мошенничество, эксплуатация доверия, социальная изоляция в цифровой среде
Обучающиеся с нарушениями слуха	Преобладание визуальных каналов коммуникации, ограниченность альтернативных источников информации	Дезинформация, вовлечение в закрытые интернет-сообщества, распространение деструктивного контента
Обучающиеся с нарушениями зрения	Зависимость от специализированных цифровых средств доступа к информации	Фишинг, вредоносное ПО, компрометация персональных данных через специализированные сервисы

Представленная классификация носит аналитический характер и предназначена для определения приоритетных направлений профилактической работы. При этом угрозы не являются строго специфичными для отдельной нозологической группы и могут проявляться у различных категорий обучающихся, однако степень их вероятности и потенциального ущерба существенно различается.

Применительно к контингенту с ОВЗ традиционная классификация угроз приобретает качественно новое наполнение. Приоритетными для данной категории являются информационно-психологические угрозы: кибербуллинг, жертвами которого обучающиеся с ментальными нарушениями становятся значительно чаще сверстников без особенностей развития; сексуальная эксплуатация, включая груминг, риск которого многократно возрастает ввиду неспособности таких обучающихся распознавать манипулятивные тактики злоумышленников; доступ к деструктивному контенту, способному нанести психологическую травму; интернет-аддикция, проявляющаяся как неконтролируемое использование цифровых устройств; а также онлайн-мошенничество, включая финансовые махинации и кражу личных данных [14].

Особую опасность данным угрозам придаёт их способность к эскалации: незначительное на первый взгляд отклонение на индивидуальном уровне при отсутствии своевременного реагирования способно закрепиться в качестве групповой нормы и в конечном счёте трансформироваться в угрозу общегосударственного масштаба. Применительно к контингенту с ОВЗ трехуровневая модель эскалации приобретает дополнительную специфику. На индивидуальном уровне когнитивные нарушения выступают факторами цифровой виктимизации, повышая вероятность для конкретного обучающегося стать жертвой обмана, травли или эксплуатации в цифровой среде. На групповом уровне наличие в учреждении

значительного числа обучающихся со схожими когнитивными особенностями создаёт среду для распространения деструктивных онлайн-практик по принципу подражания, когда один вовлечённый в рискованное поведение воспитанник становится источником угрозы для всего коллектива. На общегосударственном уровне систематическая недозащищённость наиболее уязвимой категории граждан от информационных угроз способна привести к их массовой маргинализации и исключению из социально-экономической жизни, что противоречит целям, обозначенным в Доктрине информационной безопасности [1, п. 26].

Механизмы обеспечения информационной безопасности в образовательных учреждениях. Система обеспечения информационной безопасности в образовательном учреждении опирается на три взаимосвязанных механизма: нормативно-правовой, организационно-технический и кадровый. Нормативно-правовой механизм выступает фундаментом, задавая обязательные для исполнения правила и определяя зоны ответственности. Его основу составляют три федеральных закона: № 149-ФЗ «Об информации, информационных технологиях и о защите информации», № 152-ФЗ «О персональных данных» и № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [2-4]. Для учреждений интернатного типа дополнительное значение приобретают Федеральный закон № 35-ФЗ «О противодействии терроризму» и Федеральный закон № 114-ФЗ «О противодействии экстремистской деятельности», создающие юридический фундамент для антитеррористической защищённости объектов [5; 6].

Организационно-технический механизм переводит правовые предписания в практическую плоскость. Его основу составляют средства контентной фильтрации, антивирусной защиты и криптографической защиты информации. Контентная фильтрация является центральным элементом, непосредственно вытекающим из требований 436-ФЗ. При любом варианте реализации – централизованная региональная система, локальное программное обеспечение или фильтрация на стороне провайдера – техническое ограничение доступа к запрещённым ресурсам дополняется организационными мерами: назначением ответственного, ведением журнала учёта использования интернет-ресурсов, регулярными проверками эффективности. Для учреждений интернатного типа фильтрация должна охватывать не только учебные компьютеры, но и все устройства, с которых обучающиеся могут выходить в сеть с жилой территории. Антивирусная защита обеспечивает предотвращение заражения информационных систем вредоносным программным обеспечением. Средства криптографической защиты информации приобретают особую актуальность в свете требований 152-ФЗ к защите специальных категорий персональных данных. Принципиально важно подчеркнуть, что ни одно из перечисленных средств не является самодостаточным: эффективная защита достигается только при их комплексном применении.

Кадровый механизм является связующим звеном, определяющим, насколько эффективно будут работать все остальные элементы системы. Как показывают исследования, в подавляющем большинстве случаев угрозы информационным ресурсам реализуются из-за человеческого фактора с применением методов социальной инженерии. На практике, особенно в учреждениях с ограниченным бюджетным финансированием, функции администратора информационной безопасности, как правило, исполняются сотрудником, совмещающим их с другими обязанностями. Такое совмещение порождает комплекс рисков: от нехватки квалификации до дефицита времени на мониторинг угроз и обновление средств защиты. Важнейшим элементом кадрового механизма является формирование базовых компетенций в области информационной безопасности у всех участников образовательного процесса – административного персонала, педагогических работников и самих обучающихся. Для обучающихся с ОВЗ обучение основам кибергигиены требует применения адаптированных методик, учитывающих нозологические особенности.

Роль учредителя в формировании системы информационной безопасности. Образовательные учреждения интернатного типа, подведомственные органам социальной защиты, занимают уникальное положение в системе российского публичного управления. С одной стороны, содержательные требования к образовательной деятельности, включая требования к информационной безопасности

образовательного процесса, формируются Минпросвещения России. С другой – непосредственное управление учреждением осуществляет региональное министерство социальной политики, которое утверждает штатное расписание, выделяет лимиты бюджетных обязательств и контролирует их целевое расходование. Такая ситуация порождает риск несогласованности нормативных требований и затрудняет выработку единой политики информационной безопасности.

Финансирование мероприятий по информационной безопасности в учреждениях соцзащиты характеризуется противоречием между высокими нормативными требованиями, обусловленными обработкой специальных категорий персональных данных и спецификой контингента, и ограниченностью бюджетных ресурсов. Исследования показывают, что 34% государственных организаций выделяют на ИБ до 500 тысяч рублей в год, а 9% учреждений вообще не располагают отдельными бюджетами на информационную безопасность [16]. При этом 78% организаций заявляют об остром дефиците квалифицированных ИБ-специалистов. В этих условиях критически важным становится либо выделение полноценной ставки специалиста по ИБ, либо передача части функций на аутсорсинг, либо участие учреждения в централизованных региональных программах по обеспечению информационной безопасности.

Проведённый анализ позволяет сделать несколько принципиальных выводов. Во-первых, эволюция доктринального закрепления информационной безопасности отражает возрастающее внимание государства к информационной сфере, однако недостаточная проработанность дефиниций, отсутствие актуализации Доктрины с 2016 года и отмеченные исследователями проблемы юридической техники создают ситуацию, при которой значительная часть ответственности за практическое обеспечение ИБ переносится с федерального уровня на уровень конкретных организаций. Во-вторых, специфика угроз для контингента с ОВЗ, особенно для обучающихся с ментальными нарушениями, столь существенна, что стандартные меры защиты, предписанные федеральным законодательством, не могут считаться достаточными без их адаптации к условиям конкретного учреждения.

Сформулированные выводы подтверждают необходимость перехода от теоретического осмысления проблемы к эмпирическому исследованию. Не имея детального анализа реального состояния системы информационной безопасности в конкретном учреждении интернатного типа (локальной нормативной базы, технической инфраструктуры, кадрового и финансового обеспечения), невозможно оценить, насколько существующие механизмы защиты соответствуют как доктринальным ориентирам, так и специфическим потребностям уязвимого контингента. Именно такой комплексный анализ является следующим логическим шагом и составляет предмет отдельного исследования.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 декабря 2016 г. № 646.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (действ. ред.).

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (действ. ред.).

4. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (действ. ред.).

5. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (действ. ред.).

6. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (действ. ред.).

7. Пакляченко М.Ю. Новая доктрина информационной безопасности: вопросы правовой защиты информации / М.Ю. Пакляченко // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2017. – № 2(8). – С. 96-103. – EDN ZDIIJB.

8. Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. – 2017. – № 2 (75). – С. 159-165.

9. Трусов Н.А. Правовое обеспечение информационной безопасности в современной России: от критики содержания права к правовым последствиям // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2024. – № 5. – С. 163-167.

10. Жирков Г.С., Готовцева О.Г. Основные угрозы кибербезопасности: обзор современных трендов и вызовов // Вестник науки. – 2025. – № 8 (89), Том 1. – С. 317-322.

11. Щукин Г.А. Концепция «человек – слабое звено» в информационной безопасности: проблемы и решения // Молодой ученый. – 2024. – № 22 (521). – С. 42-46.

12. Насибуллина А.Д., Королева Ю.А., Польшина М.А. Проблемы цифровой социализации подростков с ограниченными возможностями здоровья // Современное педагогическое образование. – 2023. – № 12. – С. 477-481.

13. Сидорова Г.А. Отношение подростков с интеллектуальными наяушениями (умственной отсталостью) и их родителей к вопросам безопасности в интернете // Известия Иркутского государственного университета. Серия Психология. – 2025. – Т. 52. – С. 77-87.

14. Минаев А.В. Криминология: учебное пособие для студентов юридического факультета по специальности 030501 «Юриспруденция» / А.В. Минаев, О.Н. Дубровский; Минаев А.В., Дубровский О.Н.; Тывинский гос. ун-т, каф. уголовного права и процесса. – Абакан: Бригантина, 2011. – ISBN 978-5-91178-041-8. – EDN QSGOKZ.

15. Дмитрий Геннадьевич Грибков с докладом «О новой редакции Доктрины информационной безопасности Российской Федерации». – [Электронный ресурс]. – Режим доступа: http://www.scrf.gov.ru/news/speeches/3958/.

16. Исследования «СёрчИнформ». – [Электронный ресурс]. – Режим доступа: https://itspeaker.ru/news/34-gosuchrezhdeniy-tratyat-na-ib-do-500-tys-rubley-v-god/.

FUNDAMENTALS AND SPECIFICITY OF INFORMATION SECURITY THREATS TO BOARDING EDUCATIONAL INSTITUTIONS

M.A. Lem[1], *Graduate Student*
Supervisor: *A.V. Minaev, Candidate of Legal Sciences, Associate Professor[1], Professor[2]*
[1]Kaliningrad Institute of Management
[2]Academy of Military Sciences
[1,2](Russia, Kaliningrad)

Abstract. *The article examines the evolution of the doctrinal consolidation of the concept of "information security" in the Russian Federation and its impact on the education system. Particular attention is paid to the specific characteristics of boarding-type educational institutions for persons with disabilities, which combine the functions of a vocational education organization and a social service provider. Based on an analysis of the regulatory legal framework and scientific literature, the information security threats specific to this category of students are identified and systematized, taking into account their cognitive and psycho-emotional characteristics. Drawing on this analysis, the article proposes a classification of threats by nosological groups and a three-level model of their escalation. The conclusion is drawn that the identified theoretical problems necessitate a comprehensive empirical analysis of the information security system of a specific boarding-type institution.*

Keywords: *information security; Information Security Doctrine; boarding-type educational institution; students with disabilities; mental disorders; information security threats.*