Приложение 1б.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБУЧАЮЩИХСЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Ростов-на-Дону, 2025

Методические рекомендации по основам информационной безопасности для обучающихся образовательных организаций — под общ. ред. Чурилова С. А., Москва, Ростов-на-Дону, 2024 г. — с. 21.

©Министерство образования
Ростовской области

© Национальный центр информационного противодействия
терроризму и экстремизму в образовательной среде и сети Интернет

Оглавление

[Введение 4](#_Toc206500754)

[1 Информационная безопасность как важная составляющая комплексной безопасности образовательной организации 5](#_Toc206500755)

[2 Законодательство в сфере обеспечения информационной безопасности 6](#_Toc206500756)

[3 Актуальные угрозы информационной безопасности образовательных организаций 8](#_Toc206500757)

[4 Меры обеспечения информационной безопасности образовательных организаций 10](#_Toc206500758)

[5 Рекомендации по проведению профилактических мероприятий среди обучающихся
в рамках обеспечения информационной безопасности 14](#_Toc206500759)

[6 Заключение 19](#_Toc206500760)
7 Термины и определения.………………………………………………………………………...18
8 Список рекомендованных источников.……………………………………………………………………………...................20

Введение

Обеспечение защиты обучающихся от актуальных информационных угроз – одна из приоритетных задач в рамках обучения и воспитания в современных российских общеобразовательных организация и организациях среднего профессионального образования.

Данные рекомендации разработаны с целью методического сопровождения обеспечения информационной безопасности по поручению Ростовской областной межведомственной комиссии по делам несовершеннолетних и защите их прав.

Целевая аудитория методических рекомендаций – административный и педагогический состав образовательных организаций. Документ будет полезен в работе заместителям и советникам директоров по воспитанию и взаимодействию с детскими общественными объединениями, заведующим по учебно-воспитательной части, а также преподавателям, выполняющим также функции классного руководителя.

1. Информационная безопасность как важная составляющая комплексной безопасности образовательной организации

Обеспечение комплексной безопасности образовательного пространства предполагает широкий спектр задач по исключению любых видов риска для здоровья, жизни и благополучия обучающихся, административного и преподавательского состава.

Обеспечение комплексной безопасности в общеобразовательной организации и организации среднего профессионального образования включает в себя следующие направления:

1. антитеррористическая защищенность, предполагающая внешнюю и внутреннюю безопасность для предупреждения совершения противоправных действий на территории образовательной организации. Например, установка систем видеонаблюдения, организация круглосуточной охраны территории и организация пропускного режима и т.д.;
2. пожарная безопасность, меры которой направлены на предотвращение собственно пожаров и на подготовку к возможным чрезвычайным ситуациям для защиты жизни людей и имущества. Например, разработка инструкции с действиями при пожаре; установка автоматических пожарных сигнализаций; проверка неисправностей эвакуационных путей и выходов и т.д.;
3. соблюдение санитарно-гигиенических норм для безопасности находящихся на территории людей. Например, регулярная уборка классов и коридоров; контроль качества питания и т.д.;
4. организация безопасного рабочего пространства, которое предполагает, как соблюдение норм эксплуатации здания и устранение выявленных дефектов, так создание комфортных условий труда и учебы;
5. профилактика распространение деструктивных проявлений в молодежной среде, предполагающая развитие правовой грамотности, формирование критического мышления, развенчивание деструктивных установок террористических и экстремистских организаций. К профилактической работе относится и психологическая поддержка обучающихся для своевременного выявления признаков тревожности и агрессии, а также для гармонизации обстановки в классах и группах;
6. обеспечение информационной безопасности образовательного пространства от актуальных угроз как технического (взлом сервисов), так и социального (вовлечение в совершение преступных действий) характера.

Таким образом, информационная безопасность – совокупность мер технического и социального характера, направленных на обеспечение защиты образовательного пространства от деструктивного информационно-технического воздействия. О мерах обеспечения информационной безопасности образовательного процесса пойдет речь в данных методических рекомендациях.

1. Законодательство в сфере обеспечения информационной безопасности

В Российской Федерации на протяжении последних лет выстроена адекватная угрозам нормативная правовая база, включающая в себе следующие документы:

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технология и о защите информации», определяющий понятие информации, способы ее распространения и защиты, а также основания и условия ограничения доступа к информации;

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», регулирующий сбор, хранение и обработку персональных данных граждан. Определяет порядок назначения операторов персональных данных, уведомляющих уполномоченный орган о своем статусе, а также устанавливает ответственность за нарушение принципов обработки персональных данных;

Федеральный закон от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», являющийся ключевым документом в сфере борьбы с экстремистскими проявлениями в российском обществе. Закон закрепляет перечень действий, за совершение которых предусмотрена юридическая ответственность: от демонстрации нацистской и экстремистской символики до разжигания ненависти и вражды по национальному или религиозному признаку;

Федеральный закон от 06.03.2006 г. № 35-ФЗ «О противодействии терроризму», определяющий террористическую деятельность не только как непосредственное совершение теракта, но и как информационное пособничество, финансирование, а также пропаганду идей терроризма;

Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», который определяет виды информации, запрещенные к распространению среди несовершеннолетних;

Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», определяющий базовые принципы обеспечения безопасности обучающихся и работников образовательных организаций;

Федеральный закон от 8.01.1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах», который устанавливает правовые основы контроля, производства, хранения, распространения, использования и уничтожения этих веществ, а также меры ответственности за нарушения в данной сфере с целью защиты здоровья населения и предупреждения злоупотребления наркотиками;

Федеральный закон от 14.07.2022 № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием», устанавливающий порядок регистрации таких лиц, требования по раскрытию информации о своей деятельности, а также меры по обеспечению прозрачности и безопасности национального информационного пространства;

Указ Президент Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», определяющий перечень угроз информационной безопасности России (деструктивное информационно-психологическое воздействие на население; рост преступлений, совершенных с использованием информационно-коммуникационных технологий и т.д.), направления и средства обеспечения информационной безопасности и т.д.;

Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024-2028 годы (утв. Президентом РФ 30 декабря 2023 года № Пр-2610), предписывающий комплексное проведение профилактических мероприятий общего, адресного и индивидуального характера, а также меры информационного противодействия угрозам террористического характера;

Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», устанавливающий в качестве одной из целей достижение к 2030 году «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта;

Кодекс об административных правонарушениях Российской Федерации и Уголовный кодекс Российской Федерации, устанавливающие меры за совершенные правонарушения: от ответственности за утечку персональных данных (согласно ч. 2 ст. 13.11 КоАП РФ устанавливаются штрафы на граждан, должностных лиц и организации) до содействия террористической деятельности в форме вербовки, ответственность за которое установлена в ст. 205.1 УК РФ.

Перечислены лишь основные нормативные правовые документы в области обеспечения информационной безопасности, которые необходимо знать специалистам по противодействию информационным угрозам и профилактике вовлечения молодежи в деструктивную деятельность.

1. Актуальные угрозы информационной безопасности образовательных организаций

Сегодня Россия и ее граждане ежедневно сталкиваются со значительным количеством угроз, воздействующих на общество, а также на отдельных личностей. Такие угрозы имеют как преднамеренный, умышленный характер (например, вербовка в совершение противоправных действий), так и случайные, возникающие в результате человеческого или технического фактора.

К актуальным информационным угрозам следует отнести:

1. хакерские атаки на информационные системы и кибертерроризм;
2. финансовое мошенничество;
3. распространение идеологии терроризма и экстремистских проявлений;
4. незаконный оборот наркотических средств, а также пропаганда их потребления;
5. информационно-психологические операции иностранных спецслужб, а также деятельность иноагентов и зарубежных организаций, признанных нежелательными по решению Генеральной прокуратуры Российской Федерации;
6. дискредитация традиционных российских духовно-нравственных ценностей;
7. искажение исторической памяти, распространение русофобии.

Отдельные люди, включая обучающихся и преподавательский состав, могут сталкиваться преимущественно с такими рисками и проблемами, как:

1. потеря финансовых средств в следствии мошеннических действий;
2. вовлечение в террористическую и экстремистскую деятельность: совершение терактов, оправдание и пропаганда идей террористического и экстремистского характера, вовлечение в финансирование террористических и экстремистских организаций и т.д.;
3. сбор и передача важной для безопасности информации, например, фото- и видеофиксация объектов инфраструктуры посторонним лицам;
4. кража и незаконное распространение персональных данных;
5. суицидальное и депрессивное поведение обучающихся, вызванное сложностями коммуникации и адаптации;
6. распространение компрометирующих материалов;
7. травля, в том числе в онлайн-режиме (кибербуллинг).

Важно подчеркнуть, что на основе актуальных событий, в России фиксируется несколько способов вовлечения в противоправную деятельность, в том числе террористического и экстремистского характера:

1. последствия атак мошенников, когда под воздействием угроз после перевода денег жертву принуждают к повреждению какого-либо объекта либо к иному действию (теракт, диверсия, вандализм и т.д.);
2. вступление в контакт с представителем террористической/экстремистской организации или иностранной спецслужбы для совершения противоправного действия;
3. процесс саморадикализации: по идеологическим мотивам или в силу получения финансовой выгоды.

С точки зрения создания безопасного информационного пространства
в общеобразовательных организациях и организация среднего профессионального образования администрациям образовательных организаций следует делать акцент на предотвращении таких угроз, как:

1. проникновение шпионских и вирусных программ на устройства обучающихся, преподавателей, а также в информационную инфраструктуру организации. Такие программы могут собирать личную информацию, банковские реквизиты, фото- и видеоматериалы, а также нарушить работу компьютеров и привести к потере данных;
2. информационно-психологические операции против обучающихся и педагогов, результатом которых становятся либо потеря денег или имущества, либо вовлечение в противоправную деятельность (например, незаконный митинг, поджог релейных шкафов), либо психологическое выведение человека из нормального состояния;
3. утечки баз данных об учениках и их родителях с адресами проживания, контактными телефонами и медицинскими сведениями. То же самое касается и данных административного и педагогического состава. Случайная публикация или намеренная передача данных может привести к серьезным последствиям. Например, злоумышленники могут звонить родителям обучающихся под видом сотрудников образовательной организации с просьбой «обновить данные в электронном журнале», списках учащихся или профильной системе («Сферум» и др.). Для якобы подтверждения обновления злоумышленники могут просить предупредить ребенка о том, что скоро ему будут звонить из школы. Во время общения с ребенком мошенники убеждают его назвать код из SMS-сообщения, который приходит на телефон. Этот код используется для восстановления доступа к аккаунту родителя на портале «Госуслуги» и последующих противоправных действий – от оформления микрозаймов до кражи персональных данных и иных мошеннических операций.

На сегодняшний день количество угроз, оказывающих воздействие как на общество в целом, так и на образовательные организации в частности, имеет большое многообразие. В данном разделе мы обозначили наиболее острые и актуальные проблемы, на выявление и предупреждение которых стоит обратить внимание при выстраивании системы профилактики информационных угроз. Стоит отметить, что обеспечение информационной безопасности – это комплекс мер, где на возникновение каждого вида информационной угрозы должно предусматриваться соответствующее реагирование, включая способы предупреждения. Механизмы реализации данных мер рассмотрим в следующем разделе.

1. Меры обеспечения информационной безопасности образовательных организаций

Меры по обеспечению информационной безопасности в образовательных организациях включают комплекс технических, социальных и иных действий, направленных на защиту образовательного пространства от вредного воздействия информационно-технических угроз. Ниже представлены основные направления таких мер с описанием конкретных процедур, которые помогут реализовать каждое из направлений.

1. Нормативно-правовое обеспечение.

* + разработка и внедрение локальных нормативных актов, регламентирующих вопросы информационной безопасности: правила обработки персональных данных, контроля доступа к данным, реагирования на инциденты;
	+ соответствие деятельности образовательной организации требованиям федерального законодательства (федеральных законов и других нормативных актов, перечисленных во втором разделе данных методических рекомендаций);
	+ обеспечение защиты обучающихся от нежелательной и запрещенной законом информации.

 Нормативно-правовое обеспечение создает фундаментальную правовую базу, которая позволяет системно и комплексно организовать защиту информационного пространства в образовательной организации. Это обеспечивает безопасность персональных данных и способствует сохранению психоэмоционального здоровья сотрудников и обучающихся, что является неотъемлемой частью качественного и безопасного образовательного процесса.

2. Административно-организационные меры.

* + назначение ответственных лиц и формирование службы информационной безопасности внутри организации;
	+ проведение регулярного аудита состояния информационной безопасности, выявление уязвимостей и угроз;
	+ разработка и внедрение планов реагирования на инциденты и нарушения безопасности;
	+ организация обучения и повышения квалификации сотрудников и обучающихся по вопросам информационной безопасности;
	+ формирование правил и культуры информационной безопасности среди всех участников образовательного процесса.

Формирование правил и корпоративной культуры информационной безопасности укрепляет ответственность каждого участника образовательного процесса за соблюдение установленных норм и способствует созданию безопасной и защищенной среды для обучения и работы. Таким образом, административно-организационные меры объединяют организационный, методический и кадровый аспекты, обеспечивая комплексный и устойчивый подход к обеспечению информационной безопасности образовательной организации.

3. Технические меры.

* + внедрение и эксплуатация средств технической защиты: антивирусных программ, межсетевых экранов (фаерволов), систем обнаружения и предотвращения вторжений (IDS/IPS);
	+ использование систем мониторинга безопасности (SIEM) и предотвращения утечек данных (DLP);
	+ настройка и контроль доступа к информационным ресурсам, ограничение прав пользователей;
	+ внедрение механизмов двухфакторной аутентификации и регулярная смена паролей в электронных ресурсах образовательной организации;
	+ контроль и фильтрация интернет-трафика для блокировки доступа к нежелательному и опасному контенту;
	+ организация регулярного резервного копирования данных и восстановление систем после сбоев.

Необходимо отметить, что для реализации технических мер информационной безопасности в образовательной организации требуется наличие специализированных знаний и практических навыков в области защиты информации и сетевой безопасности. Эти задачи сопровождаются высокой степенью технической сложности и требуют системного подхода к проектированию, настройке и эксплуатации средств защиты. В связи с этим в образовательной организации рекомендуется выделить специально обученного сотрудника – специалиста по информационной безопасности или системного администратора. Такой специалист должен обладать профильным образованием, знать современные технологии защиты информации, владеть навыками администрирования систем безопасности (в том числе IDS/IPS, антивирусов, средств контроля доступа и шифрования).

Кроме того, этот сотрудник отвечает за регулярное обновление и адаптацию технических мер, мониторинг угроз, проведение аудитов безопасности и обучение персонала правилам работы в безопасной среде. Без участия квалифицированного специалиста эффективное применение технических средств защиты в образовательной среде оказывается затруднено и не обеспечивает необходимый уровень безопасности.

4. Физическая безопасность.

* + ограничение доступа в помещения, где расположены серверы, базы данных и оборудование для хранения и обработки информации;
	+ оборудование помещений системами контроля доступа и видеонаблюдения;
	+ использование защищенных шкафов и сейфов для хранения документов, носителей информации и резервных копий данных;
	+ обеспечение условий безопасной эксплуатации компьютерной техники и периферийных устройств.

 Физическая безопасность является неотъемлемой частью общей системы защиты информационных ресурсов образовательной организации. В совокупности физические меры обеспечивают надежную защиту материальной базы информационной безопасности и способствуют сохранению целостности и доступности данных в образовательной организации.

 5. Образовательные и просветительские меры.

* + формирование у сотрудников и обучающихся устойчивых навыков безопасного поведения в информационной среде;
	+ включение в учебные программы дисциплин по медиаграмотности;
	+ проведение профилактических мероприятий и конкурсов по информационной безопасности среди обучающихся.

 Образовательные и просветительские меры играют ключевую роль в формировании у сотрудников и обучающихся устойчивых навыков безопасного поведения в информационной среде. Включение дисциплин по медиаграмотности в учебные программы способствует системному развитию критического мышления и способности распознавать и противодействовать информационным угрозам. Проведение профилактических мероприятий, конкурсов и игровых форматов по информационной безопасности стимулирует активное вовлечение обучающихся и повышает эффективность усвоения знаний в области информационной безопасности. Комплексный подход к образовательным и просветительским мерам создает прочную основу для формирования ответственного цифрового поведения и защиты информационного пространства образовательной организации.

6. Социально-психологические меры.

* + организация взаимодействия с психологами и социальными педагогами для поддержки обучающихся, предупреждения эмоционального и психологического давления;
	+ проведение разъяснительных работ о рисках вовлечения в противоправную деятельность через интернет;
	+ поддержка детей и подростков в ситуациях онлайн-травли, шантажа и других видов психологического давления.

 Значение мер социальной поддержки особенно велико при работе с жертвами онлайн-травли, шантажа и других видов психологического воздействия, что обеспечивает сохранение психоэмоционального здоровья и способствует созданию безопасной образовательной среды. Социально-психологические меры интегрируются в общую систему обеспечения информационной безопасности, формируя у обучающихся устойчивую защиту от информационных угроз и поддерживая их благополучие в цифровом пространстве.

Для эффективного обеспечения информационной безопасности в образовательной организации необходимо в первую очередь провести всесторонний аудит информационной инфраструктуры и всех данных, требующих защиты. Такой анализ позволяет выявить реальные слабые места и потенциальные угрозы, а также оценить эффективность уже внедренных мер безопасности. По результатам аудита требуется оперативно устранить выявленные недостатки и внедрить недостающие меры, что снизит риски информационно-технических инцидентов и обеспечит надежную защиту образовательного пространства.

Необходимо отметить, что формирование информационной безопасности образовательной организации должно включать в себя следующие субъекты:

1. Администрация образовательной организации, которая должна принять стратегические решения по обеспечению информационной безопасности, а также обеспечивать создание и поддержание благоприятной среды для работы персонала;
2. Педагогический состав, играющий ключевую роль в обучении и воспитании обучающихся. Педагоги реализуют профилактику в рамках учебного процесса, выполняют функции классного руководства, выявляют признаки подверженности информационным угрозам среди обучающихся, а также обращают внимание администрации и родителей на изменения в поведении детей;
3. Психологи и социальные работники. Данные специалисты могут предоставлять консультации и поддержку обучающимся, сталкивающимся с эмоциональными и социальными проблемами, ведь именно эмоциональная подавленность и социальные проблемы – это ключевой крючок, позволяющий злоумышленникам воздействовать на своих жертв;
4. Родительское сообщество, играющее важную роль в профилактике вовлечения в деструктивные явления. Родительское сообщество обеспечивает поддержку детям, взаимодействует с педагогами и школой, способствует профилактике деструктивного поведения и формированию безопасной среды. Ключевое значение имеет семейное воспитание: родители должны сами владеть правилами цифровой безопасности и последовательно прививать их детям, развивая критическое мышление и ответственное отношение к информации и технологиям;
5. Другие обучающиеся из числа старшеклассников, которые могут участвовать в информационно-просветительских мероприятиях и оказывать поддержку педагогам при проведении профилактической работы. Например, быть ведущими просветительских мероприятий;
6. Полиция и органы социальной защиты. В некоторых случаях образовательная организация сталкивается с ситуациями, которые выходят за рамки ее компетенций и ресурсов. Тогда необходимым становится привлечение правоохранительных органов и служб социальной защиты для профессионального разбора и решения проблемы.

Реализация изложенных в данном разделе мер способствует сохранению конфиденциальности и целостности данных, предупреждению распространения запрещенной информации, формированию у работников и обучающихся устойчивых навыков безопасного поведения в цифровой среде, а также поддержанию их психоэмоционального здоровья. Такой подход создает основу для качественного, защищенного и современного образовательного процесса, отвечающего требованиям цифровой эпохи.

1. Рекомендации по проведению профилактических мероприятий среди обучающихся в рамках обеспечения информационной безопасности

Профилактическая работа в рамках обеспечения информационной безопасности направлена, первоочередно, на развитие у обучающихся следующих компетенций:

* + развитие навыков критического мышления как ключевого инструмента по индивидуальной защите от воздействия информационных угроз;
	+ развитие психологической устойчивости и техник защиты от психологического давления;
	+ привитие обучающимся знаний о правилах информационной безопасности, касающихся защиты личных данных в интернете.

Рассмотрим каждое из обозначенных направлений в отдельности.

Критическое мышление – это навык анализировать и проверять информацию, независимо от ее источников, и делать объективные выводы для безопасного поведения. Оно помогает выявлять недостоверную информацию, не поддаваться на уловки мошенников и сохранять психологическую устойчивость. Критическому мышлению противостоит докритическое, которое предполагает следующую модель поведения: получение информации – сразу действие. Критическое же мышление предполагает между двумя обозначенными фазами проверку поступившей информации.

Критическое мышление – это инструмент, который необходимо постоянно развивать и совершенствовать каждому человеку. Нельзя утверждать, что, становясь взрослым, человек автоматически обретает навыки критического мышления.

Критическое мышление включает в себя следующие свойства:

1. Отсутствие абсолютного доверия к любой поступающей информации. Критическое мышление подразумевает сомнение в любом утверждении, особенно в тех случаях, если источник информации неизвестен либо имеет сомнительный статус. Например, если информацию распространяет личность, признанная иноагентом, или организация, признанная нежелательной по решению Генпрокуратуры Российской Федерации;
2. Умение работать с источниками информации, что подразумевает анализ поступающей информации, поиск первоисточника, оценку эмоциональности информации, анализ наличия фактических и логических ошибок и т.д.;
3. Постоянное саморазвитие, что предполагает расширение кругозора, умение решать логические задачи, а также смотреть на ситуацию с разных сторон.

Следующая составляющая, которая обеспечивает эффективное формирование информационной безопасности образовательной организации – развитие навыков защиты от психологического давления у обучающихся. Эмоционально устойчивый человек способен сохранять критическое восприятие ситуации и принимать взвешенные решения, поскольку его рациональное мышление не подавляется страхом, отчаянием или другими доминирующими эмоциями.

Психологическое давление – воздействие на человека с целью повлиять на его решения, эмоции и поведение через манипуляции, угрозы, шантаж или даже унижение. Оно может проявляться в виде угроз распространения личной информации, шантажа сообщениями или фотографиями провокационного характера, использования слабых сторон человека против него самого. Психологическое давление, часто используемое в мошеннических схемах с помощью социальной инженерии, направлено на манипулирование сознанием и поведением жертвы через эксплуатацию ее эмоций и когнитивных уязвимостей. Мошенники создают ситуации страха, паники или ложной надежды на выгоду, чтобы заставить человека совершать нужные им действия.

Среди основных признаков психологического давления можно обозначить:

* + навязывание чувства вины за отказ выполнить просьбу или требование, что снижает психологическую устойчивость и заставляет подчиняться;
	+ проявление злости, агрессии, раздражения со стороны злоумышленника для создания напряжённой атмосферы и давления;
	+ использование угроз, намёков или прямого психологического давления для запугивания и контроля;
	+ возникновение у жертвы тревоги, страха, стыда или чувства беспомощности после контакта с манипулятором;
	+ изоляция жертвы от близких или попытки контролировать её действия и коммуникации, что лишает поддержки;
	+ создание искусственного чувства срочности («у вас мало времени», «нужно действовать немедленно»), чтобы заблокировать рациональное мышление и вызвать импульсивные решения;
	+ апелляция к авторитету и официальным статусам (изображение сотрудника образовательной организации, госорганов), вызывающая безоговорочное доверие;
	+ использование многоступенчатых сценариев с разными «представителями» для подкрепления обмана;
	+ применение современных технологий (клонирование голоса, дипфейки), усиливающих достоверность манипуляций;
	+ манипуляции с обещаниями выгоды, игра на жадности, жалости, страхе потерь для побуждения к необходимым мошенникам действиям.

 Эти методы создают сложные, многослойные психологические маневры, которые затрудняют осознание обмана и требуют от пользователей высокой информационной и психологической грамотности для защиты.

 Привитие обучающимся знаний о правилах информационной безопасности, связанных с защитой личных данных в интернете, включает несколько важных аспектов. В первую очередь необходимо объяснить, что такое личные данные и почему их защита важна для безопасности каждого пользователя в цифровом пространстве. Обучающиеся должны осознавать риски, связанные с публикацией персональной информации в открытом доступе, и понимать основные правила безопасного хранения и передачи таких данных.

 В образовательном процессе следует уделять внимание методам создания надежных паролей, необходимости их регулярного обновления и использованию дополнительных способов защиты аккаунтов, таких как двухфакторная аутентификация. Особое значение имеет обучение работе с настройками приватности в социальных сетях и различных интернет-приложениях для ограничения доступа к личной информации.

 Кроме того, важно предупреждать обучающихся о мошеннических схемах и фишинговых атаках, а также формировать у них критическое отношение к запросам на предоставление персональных данных, особенно от неизвестных лиц и на сомнительных ресурсах. Обучающиеся должны знать, как действовать в случае подозрительной активности, включая обращение за помощью к взрослым или специалистам.

 Таким образом, системная передача знаний о защите личных данных способствует формированию у обучающихся грамотного и осознанного отношения к собственной цифровой безопасности и снижает риски информационных угроз в сети.

При этом необходимо учитывать, что профилактическая работа должна строиться с учетом возрастных особенностей обучающихся. Для младших школьников важно использовать простые игровые форматы и наглядные примеры, объясняя основные правила безопасного поведения в интернете доступным и понятным языком. Средние классы требуют более глубокого погружения в темы цифровой безопасности с акцентом на развитие критического мышления и умения распознавать угрозы. Для старших же учащихся необходимо применять интерактивные методы – дискуссии, дебаты, кейсы и викторины, которые способствуют формированию ответственного отношения к обработке личных данных и обеспечивают навыки противодействия современным информационным рискам. Такой дифференцированный подход позволяет максимально эффективно формировать культуру информационной безопасности, учитывая уровень восприятия и эмоциональную зрелость каждой возрастной группы.

Приведем примеры тематического наполнения занятий для обучающихся среднего звена. Для обучающихся пятого класса важно разъяснять следующие темы:

1. информация, ее виды, свойства и функции;
2. средства коммуникации и способы познания в современном информационном пространстве;
3. умение критически оценивать информацию и учиться распознавать, является ли достоверной та или иная информация, а также умение защищать собственные персональные данные надежными паролями и настройками конфиденциальности;
4. модели поведения при столкновении с недостоверной информацией, включая поиск информации из различных источников. Важно донести до сознания учеников мысль о том, что может существовать несколько правильных ответов на один вопрос.

На занятиях с обучающимися шестого класса рекомендуется делать акцент на следующих темах:

1. актуальные интернет-угрозы: распространение недостоверной информации, мошенничество, агрессия (в том числе в виде кибербуллинга), а также контент, который может причинить вред психическому здоровью (например, публикации с самоповерждениями).
2. цифровой этикет как свод правил корректного, безопасного и уважительного поведения в интернет-пространстве. К этикету относятся проявление вежливости, грамотное написание, ненарушение чужого личного пространства, а также ответственность за свои действия;
3. публикации в интернете: какие публикации можно делать, а какие не рекомендуется (включая репостинг или пересылку чужих публикаций).

С семиклассниками рекомендуется делать акцент на следующих блоках:

1. виды медиа в современном мире, через которые усваивается информация. Отдельно о роли видеоигр и о том, что их можно использовать, как и для развития мышления и познания мира, но также они могут быть и источниками опасностей. Например, что там могут действовать преступники, которые вовлекают в совершение разных противоправных действий;
2. права и обязанностей пользователей интернета: охрана собственных персональных данных и нераспространение чужих персональных данных без согласия их владельца; ответственность за распространение недостоверной информации, а также за публикации, в которых одобряется совершение каких-либо преступлений;
3. развитие навыков цифрового этикета, включая акценты на запрет разжигания ненависти и вражды по национальному, религиозному или языковому принципу.

В восьмом классе педагогам следует проводить занятия по таким темам, как:

1. продолжение развития навыков безопасного общения в интернет-пространстве, а также закрепление основных правил цифрового этикета;
2. защита от проявлений агрессии в информационно пространстве, а также привлечение к ответственности за агрессию. Особый акцент следует сделать на тематике кибербуллинга и его последствий для инициаторов травли;
3. закрепление знаний об угрозах распространения недостоверной информации, а также об ответственности за данные действия.

В просветительской работе с девятиклассниками крайне важно разъяснять следующие темы:

1. виды противоправного контента, с которым можно столкнуться в интернете;
2. актуальная опасность вербовки в противоправные и деструктивные сообщества, а также способы самозащиты от действий вербовщиков;
3. закрепление знаний об угрозах со стороны мошенников, а также разъяснение алгоритмов действий при столкновении с данной угрозой.

Рекомендуется придерживаться следующих принципов при организации профилактических мероприятий по информационной безопасности с обучающимися.

Важно говорить с обучающимися об актуальных цифровых угрозах, начиная с возраста, когда они способны воспринимать серьезную информацию, избегая излишнего травмирования. В случае чрезвычайных ситуаций (например, обеспокоенность из-за новостей) сведения о поведении в кризисных ситуациях должны быть своевременно донесены до учеников, педагогов и родителей с целью снижения паники и повышения готовности.

Не стоит подавать информацию напрямую в виде запретов или морализаторства – это может вызвать обратный эффект и заинтересовать несовершеннолетних в нежелательной теме. Лучше сосредоточиться на формировании навыков критического восприятия и безопасного поведения.

Акцент стоит делать на практических методах противодействия угрозам – обучение распознаванию мошенничества, кибербуллинга, попыток вербовки и другим опасным ситуациям, рассказывать конкретные алгоритмы действий при столкновении с опасностью: как вести себя при сомнительных звонках, попытках шантажа, подозрительных объектах или изменениях в поведении сверстников.

Приветствуется активное привлечение самих обучающихся к реализации профилактических мер, это способствует созданию атмосферы коллективной ответственности и объективного восприятия рисков.

Для старших классов особенно рекомендуется проведение соревновательных мероприятий по информационной безопасности. Положительным примером можно привести опыт проведения онлайн-олимпиад по медиабезопасности Автономной некоммерческой организацией цифровой ресурсный центр поддержки некоммерческого сектора «Интернет без угроз». Данные олимпиады АНО «Интернет без угроз» проводятся с 2020 года. В 2024 году блоки олимпиады касались вопросов защиты персональных данных, ответственности за вовлечение в разные противоправные действия через интернет, вопросов определения применения искусственного интеллекта в создании визуально контента (определение дипфейков). Участниками олимпиады стали 6486 старшеклассников.

Старшеклассников также можно привлекать к просветительской работе по теме медиаграмотности и информационной безопасности среди сверстников и младшеклассников. Например, такой деятельностью занимаются выпускники информационно-просветительского проекта «Инспектора медиабезопасности». Данное сообщество добровольцев в сфере медиабезопасности зарекомендовало себя как эффективная практика просветительской деятельности.  «Инспектора медиабезопасности» – проект по обучению старшеклассников методикам распространения среди молодежи основ медиаграмотности, критического мышления и информационной безопасности. По итогам обучения участники готовят собственные уроки, которые проводят в общеобразовательных организациях и организация среднего профессионального образования. Проект реализуется в Ростовской области с 2023 года, за этот период основам медиабезопасности обучено 45 старшеклассников и студентов СПО Ростовской области, которые своими просветительскими мероприятиями охватили более 800 сверстников, создали профилактический контент по теме и выступили соавторами нового социально-значимого проекта по медиабезопасности для несовершеннолетних (Интернет-шоу «Переменка»).

«Интернет-шоу «Переменка» – еще одна успешная практика привлечения старшеклассников к просветительской деятельности. Проект представляет собой серию видеороликов в формате интернет-шоу, где старшеклассники в роли ведущих обсуждают актуальные темы медиабезопасности с приглашенными экспертами[[1]](#footnote-1). Проект стремится не только информировать подростков о возможных опасностях в интернете, но и дать им инструменты для их предотвращения. Применяя принцип «равный-равному», создается пространство, где подростки-зрители могут услышать полезные рекомендации от своих ровесников, что делает информацию более доступной и повышает уровень доверия к ней. В настоящее время снято 5 эпизодов, фрагменты которых можно использовать при проведении занятий с обучающимися.

Необходимо помнить, что профилактическая работа имеет комплексный характер, включает в себя большое количество субъектов, а также предполагает использование современных форматов реализации мероприятий. Применение новых технологий и медиаформатов делает профилактику более привлекательной и доступной для обучающихся, позволяя формировать у них устойчивые навыки информационной безопасности и критического мышления.

1. Заключение

Обеспечение информационной безопасности образовательной организации – важная составляющая общей системы безопасности организации. Меры по обеспечению информационной безопасности в образовательных организациях представляют собой комплексный и взаимосвязанный набор действий, включающий нормативно-правовое регулирование, административное управление, техническую защиту, физическую безопасность, а также образовательные, просветительские и социально-психологические мероприятия.

Комплексный подход к реализации этих мер позволяет создать безопасное информационное пространство, в котором обеспечивается защита персональных данных, предупреждаются информационные угрозы, поддерживается психоэмоциональное благополучие обучающихся и сотрудников.

В основе успешной защиты лежит проведение регулярного аудита информационной инфраструктуры, выявление уязвимостей и оперативное устранение несоответствий, что обеспечивает актуальность и надежность применяемых мер. Важную роль играет компетентный персонал, отвечающий за техническую и организационную безопасность, а также активное участие всех субъектов образовательного процесса – от администрации до самих обучающихся.

1. Термины и определения

IDS (Intrusion Detection System) – система обнаружения вторжений. Это программный или аппаратный комплекс, который постоянно мониторит сетевой трафик и действия
в информационной системе с целью выявления подозрительной активности или попыток несанкционированного доступа. IDS фиксирует потенциальные угрозы и оповещает об этом администраторов, но не блокирует атаки самостоятельно.

IPS (Intrusion Prevention System) – система предотвращения вторжений. Это более продвинутая система, которая не только обнаруживает подозрительную активность, но и автоматически предпринимает меры для блокировки атак, например, разрывает соединения со злоумышленниками или блокирует вредоносный трафик в реальном времени.

Дипфейк – это технология создания поддельных аудио- или видеоматериалов с использованием методов искусственного интеллекта и глубокого обучения, которая позволяет создавать реалистичные фальшивые изображения и записи голосов людей. Такие материалы могут имитировать поведение, мимику или речь конкретного человека, вводя в заблуждение зрителей и слушателей.

Социальная инженерия – метод манипулирования людьми с целью получения конфиденциальной информации или доступа к защищенным системам. Злоумышленники используют психологические приемы, обман и знание человеческой психологии, чтобы побудить жертв раскрыть пароли, передать доступы или установить вредоносное программное обеспечение.

Фишинг – вид интернет-мошенничества, основанный на использовании методов социальной инженерии, направленный на кражу конфиденциальной информации пользователей. Мошенники маскируются под доверенные источники, такие как банки, государственные учреждения или популярные сервисы, и обманывают пользователей, заставляя их раскрывать личные данные (логины, пароли, номера банковских карт) через фальшивые электронные письма, сообщения или сайты.

1. Список рекомендованных источников

Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10 апреля 2020 г. № ЛБ-С-088-8929 «О направлении методических рекомендаций»: https://clck.ru/3NsCoF

Памятка для обучающихся, родителей (законных представителей) и педагогических работников по вопросам противодействия травле (буллингу): https://clck.ru/3NsCmW

Комикс, разработанный НЦПТИ, раскрывающий маркеры вербовщика и правила защиты от вербовки для обучающихся («Заявка в друзья»): <https://clck.ru/3NjdLk>

Комикс, разработанный НЦПТИ, обучающий детей настраивать собственную новостную ленту и защищаться от негативного контента («Публикация в сети»): https://clck.ru/3NjfPy

Информационный материал, разработанный АНО «Интернет без угроз», «Пять мифов о медиабезопасности»: https://clck.ru/3NsETo

Информационный материал, разработанный АНО «Интернет без угроз», «Правила надежного пароля»: https://clck.ru/3NsEU9

Информационный материал, разработанный АНО «Интернет без угроз», «Как распознать фишинговое письмо»: <https://clck.ru/3NsEWV>

Информационный материал, разработанный АНО «Интернет без угроз», «Опасные челленджи в интернете»: https://clck.ru/3NsEXQ

Информационный материал, разработанный АНО «Интернет без угроз», «Ребенок
и кибергрумминг»: https://clck.ru/3NsEXh

1. Ссылка на видеоролики: https://clck.ru/3NjhWF [↑](#footnote-ref-1)