Государственное бюджетное профессиональное образовательное учреждение
«ВОЛГОГРАДСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

Учтено мнение

Совета обучающихся ГБПОУ ВИТ
Протокол № 3
от 18 июня 2026

Совета родителей ГБПОУ ВИТ
Протокол № 4
от 18 июня 2026

УТВЕРЖДАЮ
Директор ГБПОУ «Волгоградский индустриальный техникум»
_____ В.Е. Древин
23 июня 2026 г.

ПОЛОЖЕНИЕ
о деятельности кибердружины «Курсив» ГБПОУ «Волгоградский индустриальный техникум»

Рег. номер 312 от 23 июня 2026 года
Введено в действие приказом директора
№ 274-ОД от 23 июня 2026 года

2026 г.

1.Общие положения

1.1. Настоящее Положение определяет цели, задачи, порядок деятельности кибердружины.

1.2. Настоящее Положение разработано в соответствии с законодательством Российской Федерации и Волгоградской области в сфере информационной безопасности, защиты детей от противоправного контента, добровольческой (волонтёрской) деятельности, о противодействии экстремистской деятельности, а также профилактики безнадзорности и правонарушений несовершеннолетних.

2. Цель и задачи деятельности кибердружины

2.1. Целью деятельности кибердружины является противодействие распространению в сети Интернет противоправной информации и профилактика негативных явлений среди обучающихся.

2.2. Для достижения поставленной цели необходимо решение следующих задач:

информирование участников образовательного процесса о необходимых действиях при обнаружении противоправной информации в сети Интернет;

выявление признаков деструктивного (девиантного) поведения среди обучающихся;

выявление фактов распространения информации, склоняющей обучающихся к асоциальному поведению, причиняющей психологический и физический вред здоровью и развитию обучающихся;

осуществление специальной подготовки, обучение участников кибердружины;

содействие государственным структурам в борьбе с размещенной в сети Интернет информацией, распространение которой в Российской Федерации запрещено;

организация информационно-разъяснительной и агитационно-пропагандистской работы по привлечению новых участников в кибердружину;

создание информационной продукции (совместно с медиа центрами), поддержка комфортной и безопасной среды в сети Интернет.

3. Направления деятельности

3.1. Просветительская деятельность киберволонтеров.

3.1.1. Добровольческая (волонтерская) деятельность в области образования/образовательное волонтерство включает участие и содействие квалифицированных добровольцев (волонтеров) в реализации просветительских программ и проектов, а также в развитии дополнительных компетенций для детей и взрослых. Данный вид деятельности может реализовываться, в том числе через осуществление просветительской и консультативной деятельности,

наставничества, тьюторства, в формате "обучение через добровольчество (волонтерство)", предполагающем участие преподавателей и обучающихся в добровольческих (волонтерских) проектах и программах образовательных организаций всех уровней образования, реализации совместных благотворительных программ образовательных организаций, социально ориентированных некоммерческих организаций и коммерческих организаций с использованием их профессиональных компетенций.

3.1.2. Формами реализации просветительской деятельности киберволонтеров являются:

проведение занятий, лекций, мастер-классов по вопросам информационной безопасности, цифровой грамотности, безопасного поведения в сети "Интернет";

разработка и распространение информационных материалов (памятки, буклеты, видеоролики) по противодействию деструктивной идеологии;

организация и участие в мероприятиях, направленных на сохранение и укрепление традиционных российских духовно-нравственных ценностей.

3.1.3. Добровольческая (волонтерская) деятельность в сфере информационного освещения и поля вокруг общественно значимых событий, информационную поддержку социальных и добровольческих проектов, мероприятий и программ; создание волонтерами в качестве фотографов, журналистов, SMM-специалистов, видеооператоров позитивного, профилактического контента и его распространение в СМИ и социальных сетях.

3.2. Мониторинг общедоступных источников киберволонтерами.

3.2.1. Мониторинг осуществляется в целях выявления противоправного контента в открытых группах, каналах, пабликах, форумах с фиксацией ссылок на выявленный контент, и направлением информации в уполномоченные органы в порядке согласно Приложению 6 к настоящему Положению.

3.2.2. Мониторинг киберволонтерами осуществляется исключительно в отношении общедоступных источников. Доступ к закрытым каналам связи (мессенджеры, чаты с ограниченным доступом, закрытые профили) не допускается.

Добровольчество в сфере мониторинга сети "Интернет" на предмет выявления противоправных материалов: мониторинг, сбор, анализ ссылок на материалы и передачу в органы власти и правоохранительные органы для реагирования на выявленные информационные угрозы. Анализ социальных сетей, мессенджеров, видеохостингов, ресурсов для видеотрансляций, игровых онлайн-платформ и других площадок (страниц пользователей, чатов, групповых чатов, телеграм-каналов, форумов) является инструментом профилактики и предупреждения вовлечения детей и молодежи в деструктивное (в том числе девиантное) поведение.

В зависимости от целей и задач существования киберволонтерской организации мониторинг может осуществляться по всем или одному тематическому направлению поиска противоправного контента: суицидальное

поведение; вооруженные нападения на образовательные учреждения (скулшутинг, "Колумбайн"); межнациональные отношения; М.К.У.; анархизм (критика власти); криминальные субкультуры; пропаганда употребления наркотиков; "околофутбол" (футбольное хулиганство); потенциальные диверсии; нацизм.

Запрещается:

мониторинг закрытых каналов связи (мессенджеры, чаты с ограниченным доступом);

сбор персональных данных лиц, разместивших контент, без согласия (за исключением случаев, предусмотренных ст. 6 ч. 1 п. 2–11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных");

самостоятельное блокирование, удаление или ограничение доступа к выявленному контенту.

3.3. Консультативная деятельность киберволонтеров.

3.3.1. Консультативная деятельность.

Формы реализации:

консультирование граждан по вопросам защиты от мошенничества в сети "Интернет";

разъяснение порядка действий при обнаружении противоправного контента;

информирование о способах ограничения доступа к деструктивной информации.

3.4. Информационная поддержка населения киберволонтерами.

Формы реализации:

создание и распространение позитивного контента, направленного на популяризацию традиционных ценностей;

информационное сопровождение мероприятий в сфере молодежной политики и профилактики деструктивных проявлений.

3.5. Добровольчество (волонтерство) в сфере реализации профилактических мероприятий. Включает оказание безвозмездной помощи в подготовке, проведении и достижении стратегических целей какого-либо профилактического мероприятия и осуществляется на различных мероприятиях локального, местного, регионального, федерального и международного уровней.

4. Порядок организации кибердружины

4.1. Директор государственного бюджетного профессионального образовательного учреждения «Волгоградский индустриальный техникум» утверждает Положение о деятельности кибердружины, назначает ее координатора.

4.2. Координатор кибердружины проводит организационное собрание с кандидатами в киберволонтеры, на котором формируется кибердружина образовательной организации.

На организационном собрании осуществляется регистрация участников, ведется протокол, принимаются заявления киберволонтеров, согласия

на обработку персональных данных, заключается договор с киберволонтерами, проводятся инструктажи с обязательным документированием их проведения, рассматриваются вопросы обучения киберволонтеров и др.

4.3. Состав кибердружины определяется приказом директора техникума. Участники кибердружины осуществляют свою деятельность на принципах законности, добровольности, личной и социальной ответственности.

5. Порядок деятельности кибердружины

5.1. Кибердружина осуществляет мониторинг сети Интернет с целью выявления следующей информации о негативных, кризисных и проблемных социальных явлениях в детской и молодежной среде, в том числе причиняющей вред здоровью и (или) развитию детей и подростков; включенной в федеральный список экстремистских материалов; содержащей признаки призывов к самоубийству, пропаганды наркотиков, детской порнографии, азартных игр; о чрезвычайных происшествиях; сведениях о преступлениях и правонарушениях, в числе которых преступления в отношении детей и подростков, а также совершенные самими несовершеннолетними; публикации и комментарии провокационного характера, просьбы о помощи, включая психологическую.

5.2. Кибердружина осуществляет мониторинг по различным тематическим направлениям поиска противоправного контента, в том числе: суицидальное поведение; вооруженные нападения на образовательные учреждения; межнациональные отношения; М.К.У.; анархизм (критика власти); криминальные субкультуры; пропаганда употребления наркотиков; околофутбол (футбольное хулиганство); потенциальные диверсии; нацизм и другие.

5.3.Мониторинг осуществляется киберволонтерами на предмет выявления противоправных материалов: социальных сетей, мессенджеров, видеохостингов, ресурсов для видеотрансляций, игр, и других площадок (страниц пользователей, чатов, групповых чатов, каналов, форумов).

5.4. Виды мониторинга:

первичный – мониторинг всех обучающихся в начале учебного года;

периодический – мониторинг всех обучающихся 1 раз в квартал;

профилактический – мониторинг обучающихся, требующих дополнительных профилактических мер и постоянного мониторинга социальной активности проводится ежемесячно;

внеплановый – мониторинг обучающихся, выявленных из внешних источников (например, компетентными органами, центром управления регионом Волгоградской области, региональным ресурсным центром информационной безопасности и цифровой грамотности детей (РЦИБ) государственного бюджетного образовательного учреждения высшего образования "Волжский институт экономики, педагогики и права" (ГБОУ ВО "ВИЭПП") и иными компетентными структурами) проводится при поступлении информации.

5.5. Киберволонтеры осуществляют мониторинг согласно алгоритму:

Этап 1: Анализ контента.

Первый шаг – это сбор и изучение всей доступной информации личной страницы пользователя. Особое внимание уделяется следующим элементам профиля:

Главное фото (аватар) и обложка страницы, которые могут содержать изображения с признаками насилия, оружия или известных личностей, связанных с массовыми убийствами (скулшутеры, суициденты).

Личные данные, указанные пользователем: имя, фамилия, город проживания, интересы, род деятельности и другие сведения, которые могут помочь в составлении психологического портрета и понимании его социальной ситуации.

Текстовые публикации, репосты и комментарии, музыка, видеоконтент, которые могут выражать симпатии к деструктивным явлениям или личностям, содержать скрытые или открытые призывы к насилию и суициду.

Второй шаг – наблюдение за внешними изменениями (маркерами).

В рамках нахождения в образовательной организации: изменение поведения (замкнутое, резкое и грубое, вспыльчивое или подавленное и др.); жалобы на плохое самочувствие; пропуски занятий; внезапное или постепенное снижение успеваемости; резкая смена речи и круга тем (появление в речи жаргонной и ненормативной лексики, сленговых слов и др.); подозрительная активность в Интернете; изменение в стиле одежды, внешнем виде; появление атрибутики; избегание сверстников и педагогов; высказывание мыслей агрессивного характера и другое.

В рамках общения с родителями (законными представителями): дома появляется символика, атрибуты, предметы, которые могут быть использованы как оружие; увеличивается время нахождения за компьютером, увлечение художественной литературой, фильмами, компьютерными играми с признаками экстремистко-политического содержания, на компьютере сохранены ссылки/ файлы с текстами, ролики, изображения экстремистко-политического содержания.

Этап 2: Классификация уровня риска.

На основании анализа контента определяется уровень потенциальной угрозы, которую пользователь представляет для себя и окружающих:

Нулевая степень риска характеризуется отсутствием потенциальной угрозы. Меры не принимаются.

Низкая степень риска характеризуется следующим: минимальные проявления деструктивного интереса, не требует срочного вмешательства, материалы передаются в компетентные органы для проведения психолого-педагогического сопровождения. Низкая степень риска в данном контексте представляет собой категорию сообщений и высказываний, которые могут вызывать беспокойство или подозрения, но не содержат прямых и конкретных угроз применения насилия в отношении себя и других лиц, призывов к насилию, пропаганды насильственной идеологии, оправдания насилия, возбуждения ненависти в отношении любой группы лиц.

К низкой степени риска относятся профили, у которых на странице содержатся только графические признаки без текста: изображения известных серийных и массовых убийц, известных суицидентов, изображения оружия, изображения с признаками насилия, изображения, косвенно указывающие на вовлеченность в тематику скулшутинга (творчество на тему скулшутинга, кадры из фильмов про скулшутинг, мемы про скулшутинг) и суицида (предметы для совершения суицида творчество на тему суицида). Высказывания, вызывающие тревогу или подозрения, однако не содержащие прямых угроз ("Мне не хочется жить", "Я чувствую себя на краю пропасти"). Упоминания о суицидальных мыслях и переживаниях, не сопровождающиеся явными декларациями о намерениях. Цитаты массовых убийц или обсуждение событий массовых нападений без призыва к действиям.

Отчет координатора кибердружины передается заместителю директора по учебно-воспитательной работе для принятия профилактических мер и проведения диагностического минимума для подтверждения/опровержения наличия деструктивного поведения.

Высокая степень риска отражает высокий уровень потенциальной опасности, наличие выраженной вовлеченности в деструктивные темы и(или) планов совершить насильственные действия. Высокая степень риска представляет собой категорию сообщений и высказываний, которые содержат прямые и конкретные угрозы применения насилия в отношении себя и других лиц, призывы к насилию, пропаганду насильственной идеологии, оправдание насилия, возбуждение ненависти в отношении любой группы лиц.

К высокой степени риска относятся профили, у которых на странице содержатся как графические признаки, так и текстовые признаки:

прямые и конкретные угрозы в отношении других людей, учебных заведений или публичных мест ("устрою резню", "будет бойня");

выражение восхищения или подражания известным преступникам и призывы к повторению их действий ("будь как Харрис", "хочу устроить Керчь2.0");

положительное отношение к суициду и четко выраженные намерения его совершения ("сегодня последний день моей жизни", "я купил все необходимые таблетки").

Отчет координатора кибердружины передается директору техникума и в компетентные органы для принятия оперативных мер реагирования.

5.6. Координатор кибердружины готовит информационную справку о результатах мониторинга социальных сетей, каналов и других ресурсов обучающихся 1 раз в квартал и направляет ее заместителю директора/проректору по воспитательной работе и молодежной политике либо другому ответственному лицу в образовательной организации.

5.7. Заместитель директора по учебно-воспитательной работе готовит сводную информацию для директора техникума, корректирует план воспитательной работы, планирует профилактические мероприятия, организует

работу с активом обучающихся.

5.8. Координатор кибердружины по согласованию с руководителем образовательной организации готовит информационную справку о результатах мониторинга социальных сетей, каналов и других ресурсов обучающихся.

5.9.Результаты мониторинга рекомендуется учитывать при корректировке планов воспитательной работы, планировании профилактических мероприятий, организации работы с активом обучающихся.

5.10. Кибердружина участвует в создании информационной продукции (совместно с медиа-центром), поддержке комфортной и безопасной среды в сети Интернет согласно плану воспитательной работы.

6. Компетенции киберволонтера

6.1 Требования к кандидатам в киберволонтеры:

возраст от 18 лет (совершеннолетние граждане), наличие опыта реализации социальных проектов и иной волонтерской деятельности кандидата, наличие у него навыков работы в команде, коммуникационных компетенций, навыки создания контента, способность критически мыслить и перепроверять информацию.

Членами кибердружины могут быть педагогические работники, в том числе кураторы учебных групп, педагог-психолог, социальный педагог и иные педагогические работники; заведующие кафедрами, заместитель директора по учебно-воспитательной работе, советник директора по воспитанию и взаимодействию с детскими общественными объединениями, специалисты/члены медиа-центров, обучающиеся образовательной организации и представители родительской общественности в учебной группе.

6.2. Мониторингом сети Интернет на предмет выявления противоправного контента могут заниматься совершеннолетние граждане Российской Федерации, прошедшим обучение на курсах повышения квалификации по процессам проверки достоверности и точности информации.

7. Права и обязанности участников кибердружины.

7.1. Участники кибердружины имеют право:

участвовать во всех мероприятиях, проводимых кибердружиной;

вносить предложения по вопросам, связанным с повышением эффективности деятельности кибердружины;

получать информацию о планируемых мероприятиях;

создавать собственные киберволонтерские проекты;

добровольно выйти из состава кибердружины.

7.2. Участники кибердружины обязаны:

соблюдать законодательство Российской Федерации и Волгоградской области, настоящее Положение в рамках своей деятельности;

оказывать содействие в организации и проведении мероприятий,

проводимых кибердружиной;

уважать интересы интернет-пользователей, соблюдать этические нормы и требования законодательства при осуществлении своей деятельности;

осуществлять поиск интернет-ресурсов, содержащих противоправную информацию, а также информацию, способную причинить вред здоровью и развитию личности подростков;

сообщать информацию о выявленном противоправном контенте координатору кибердружины;

участвовать в создании позитивного контента, поддержке комфортной и безопасной среды в сети Интернет.

8. Внесение изменений и дополнений в настоящее Положение

8.1 Внесение изменений и дополнений в настоящее Положение осуществляется путем подготовки проекта Положения в новой редакции руководителем кибердружины.

8.2 Утверждение вносимых изменений и дополнений в Положение осуществляется после принятия решения Координационным советом с последующим утверждением Положения локальным правовым актом (приказом, распоряжением) директора техникума.

8.3 Кибердружина создается, ликвидируется, реорганизуется и переименовывается исключительно локальным правовым актом директора техникума.

Заместитель директора
по учебно-воспитательной работе И.В. Двинянинаа

Согласовано:
Юрисконсульт

И.В. Гайдадина

Приложение 1

Заявление о принятии в состав кибердружины
(на бланке организации-организатора)

Координатору кибердружины

_____
(наименование организации)

от _____
(фамилия, имя, отчество полностью)

ЗАЯВЛЕНИЕ

Прошу принять меня в состав кибердружины для осуществления добровольческой (волонтерской) деятельности в соответствии с Положением о киберволонтерской деятельности в образовательных организациях Волгоградской области.

С видами деятельности, правами и обязанностями киберволонтера, а также с перечнем запрещенных действий ознакомлен(а) и обязуюсь их соблюдать.

О себе сообщаю следующие сведения:
ФИО
дата рождения
паспортные данные
адрес регистрации по месту жительства
контактный телефон
адрес электронной почты
место работы/учебы.

С Политикой обработки персональных данных в

_____
(наименование организации-организатора)
ознакомлен(а) и согласен(на) с её положениями.

Приложение:
1. Копия паспорта на ___ л.
2. Согласие на обработку персональных данных на ___ л.

Дата «___» _____ 20__ г.
Подпись _____ /_____/
(расшифровка подписи)

Приложение 2

Координатору кибердружины
(ФИО волонтера)
_____

Дата рождения_____
проживающего (ей) по адресу:
_____

паспорт: серия_____ номер_____
кем и когда выдан
_____
место работы/учебы
_____
номер телефона

Согласие на обработку персональных данных

Выражаю согласие на обработку моих персональных данных в целях информационного обеспечения добровольческой (волонтёрской) деятельности, включая выполнение действий по сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению), распространению (в том числе передаче) и уничтожению моих персональных данных.

Вышеприведенное согласие на обработку моих персональных данных представлено в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", согласно которому обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения Соглашения (договора) о добровольческом (волонтёрском) труде, Стороной в котором я являюсь, может осуществляться без моего дополнительного согласия.

Настоящее согласие вступает в силу с момента его подписания и выдачи личной книжки добровольца (волонтёра) или на срок действия Соглашения (договора) о добровольческом (волонтёрском) труде *(наименование благополучателя)* организацией (учреждением), привлекающей добровольцев (волонтеров) и может быть отозвано путем подачи письменного заявления.

дата подпись ФИО

Приложение 3

Согласие законного представителя обучающегося на обработку его персональных данных образовательной организации

Я,_____,
(фамилия, имя, отчество)
паспорт: серия _____№ _____ выдан _____
_____
(кем и когда выдан)
зарегистрирован (а) по адресу:_____
_____,
являюсь законным представителем несовершеннолетнего обучающегося
_____
(Ф.И.О. несовершеннолетнего, дата рождения полностью)
на основании _____
_____
(наименование документа, подтверждающего, что субъект является законным представителем
_____
обучающегося, например, свидетельство о рождении: дата, номер и кем выдан)
действуя по собственной воле и в интересах своего ребенка даю свое согласие образовательной организации:
_____
(наименование образовательной организации, юридический адрес)
_____
_____
на использование способами, не противоречащими законодательству Российской Федерации, моих персональных данных и персональных данных моего ребенка _____
(фамилия, имя, отчество ребенка)
в связи с участием в киберволонтерской деятельности на следующих условиях:

я соглашаюсь на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), в том числе государственным органам, обезличивание, блокирование, удаление, уничтожение) для осуществления действий, предусмотренных законодательством Российской Федерации, следующих персональных данных:

фамилия, имя, отчество, пол, дата рождения;

контактная информация (номер телефона, адрес электронной почты);

портретная фотография (фото из личного дела);

документы, удостоверяющие личность обучающегося (свидетельство о рождении или паспорт), гражданство;

место регистрации по месту жительства, состав семьи;

информация о родителях (законных представителях) обучающегося

(фамилия, имя, отчество, контактная информация, паспортные данные);

места предыдущей учебы;

информация об успеваемости и посещаемости занятий, о результатах промежуточной и итоговой аттестации;

информация об участии и результатах участия в олимпиадах, конкурсах, соревнованиях, конференциях и т.д.;

полис медицинского страхования, документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для обучения в образовательной организации конкретного вида и типа, о возможности изучения предметов, представляющих повышенную опасность для здоровья и т.п.);

СНИЛС, документы, подтверждающие право на дополнительные гарантии, компенсации по определенным основаниям, предусмотренным законодательством (многодетная семья, родители-инвалиды, неполная семья, ребенок-сирота и т.п.);

данные об открытом расчетном счете;

характеристика обучающегося, в том числе отношение к "группе риска", сведения о совершении правонарушений, постановке на учет в органах и учреждениях системы профилактики безнадзорности правонарушений несовершеннолетних;

иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления обучающемуся социальных и иных гарантий, компенсаций, установленных законодательством).

Персональные данные в составе заявки могут быть переданы третьим лицам – региональному оператору киберволонтерской деятельности.

Иное разглашение персональных данных моего ребенка может осуществляться только с моего письменного согласия.

Я ознакомлен(-а) с тем, что:

согласие на обработку персональных данных действует с даты подписания настоящего согласия;

согласие на обработку персональных данных может быть отозвано мной на основании письменного заявления в произвольной форме;

в случае отзыва согласия на обработку персональных данных организация вправе применить положение части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных";

мои персональные данные будут храниться в организации в течение предусмотренного законодательством Российской Федерации срока хранения документов.

"___"_____ 20 г. _____ _____

(подпись) (фамилия, инициалы)

Приложение 4

ИНФОРМАЦИОННАЯ СПРАВКА
о результатах мониторинга социальных сетей и каналов обучающихся
_____месяц

курс

Количество обучающихся: _____
Проверено аккаунтов обучающихся (с указанием социальной сети): ____
Проверка осуществлялась методом педагогического наблюдения и анализа социальных сетей и каналов обучающихся.

Результат: *Материалы, размещенные на страницах обучающихся проверены – запрещенные материалы и группы не выявлены. Среди фото, видео- и аудио материалов, размещенных на страницах обучающихся, подозрительных не обнаружено.*

В случае выявления фактов принадлежности к деструктивным группам заполняется таблица.

№	ФИО обучающегося	Категория учета	Ник в сети	Адрес страницы в сети (указать социальную сеть)	Отметка о принадлежности к деструктивным и асоциальным группам в социальной сети или на канале

"____" _____20___г.

Куратор учебной группы _____ /И.О. Фамилия/
подпись

Приложение 5

АЛГОРИТМ
передачи информации в правоохранительные органы

Шаг №1.

Киберволонтер, осуществляя мониторинг в целях выявления противоправного контента в открытых группах, каналах, пабликах, форумах, выявляет/получает информацию о цифровом деструктивном событии, устанавливает владельца указанного профиля (деанонимизация).

Киберволонтер осуществляет мониторинг согласно утвержденному алгоритму в соответствии с этапами.

Этап 1: Анализ контента.

Первый шаг – это сбор и изучение всей доступной информации личной страницы пользователя.

Второй шаг – наблюдение за внешними изменениями (маркерами).

Этап 2: Классификация уровня риска.

Шаг №2.

Киберволонтер передает отчет координатору кибердружины в организации-организаторе киберволонтерской деятельности о выявленном цифровом деструктивном событии при установлении высокой степени потенциального риска координатору кибердружины в течение 1-го дня с момента выявления.

Шаг №3.

Киберволонтер и координатор кибердружины осуществляют проверку полученных сведений (проводят анализ информации, маркеров) и, в случае подтверждения высокой степени потенциального риска, координатор кибердружины в течение 1-го дня с момента подтверждения направляет полученную информацию в форме справки о результатах анализа профиля руководителю образовательной организации и в компетентные органы для принятия оперативных мер реагирования.

Шаг №4.

Руководитель образовательной организации немедленно направляет полученную информацию в форме справки о результатах анализа профиля региональному оператору киберволонтерской деятельности на территории Волгоградской области - региональному ресурсному центру информационной безопасности и цифровой грамотности детей (ЦИБ) государственного бюджетного образовательного учреждения высшего образования "Волжский институт экономики, педагогики и права" (ГБОУ ВО "ВИЭПП") для ведения

статистического учета базы данных деструктивных проявлений в молодежной среде на территории региона и методического сопровождения адресно-профилактической работы в образовательной организации по выявленному случаю.

Шаг №5.

Правоохранительный орган отрабатывает полученную информацию о выявленном риске в соответствии с требованиями законодательства Российской Федерации, представленными полномочиями и компетенцией.