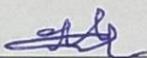


государственное бюджетное общеобразовательное учреждение
Самарской области основная общеобразовательная школа №2
городского округа Отрадный Самарской области

Рассмотрено

Зам. директора по ВР

Кострюкова О.А.



30 августа 2021 г.

Согласовано

Зам. директора по УВР

Моисеева Н.Н.



30 августа 2021 г.

Утверждаю

и. о. директора ГБОУ ООШ №2

Моисеева Н.Н.



приказ № 225-П 30 августа 2021 г.



Программа внеурочной деятельности

«Цифровая гигиена»

модуль 1 «Информационная безопасность»

направление: общеинтеллектуальное

9 класс

срок реализации: 1 год

составитель: Ворошилова Наталья Сергеевна, учитель I квалификационной категории

Отрадный, 2021

Пояснительная записка

Нормативная база программы:	<ul style="list-style-type: none">• Закон РФ «Об образовании в Российской Федерации» № 273-ФЗ от 29.12.2012;• Федеральный государственный образовательный стандарт основного общего образования (Приказ Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897, в редакции приказа Министерства образования и науки РФ от 29.12.2014 г. № 1644, от 31 декабря 2015 г № 1577);• Примерная основная образовательная программа основного общего образования, одобренная решением федерального учебно-методического объединения по общему образованию (протокол от 8 апреля 2015 г. № 1/15);• Перечень организаций, осуществляющих выпуск учебных пособий, которые допускаются к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования, утвержденный приказом Минобрнауки РФ от 09.06.2016 № 699;• Основная образовательная программа основного общего образования ГБОУ ООШ №2 г.о. Отрадный;• Программа для общеобразовательных учреждений Информатика 2-11 классы. – М.: БИНОМ. Лаборатория знаний, 2015г.• Информатика. Методическое пособие для учителя Авторы: Бородин М. Н. Год издания: 2015.• Примерная рабочая программа учебного курса «Цифровая гигиена», рекомендованная координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол №27 от 21.08.2019).
Общее количество часов:	34 часа
Уровень реализации:	9 класс
Срок реализации:	1 год
Автор(ы)работы программы:	Ворошилова Наталья Сергеевна

Программа адаптирована для школы, в которой в условиях инклюзии обучаются дети с ОВЗ, которым ПМПК рекомендовала обучение по адаптированной образовательной программе для детей с ЗПР (вариант 7.1), а также дети со школьными трудностями различного характера.

Программа курса «Цифровая гигиена» адресована учащимся 9 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

Основными целями изучения курса «Цифровая гигиена» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и, ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании курса «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

Место учебного курса в учебном плане

Программа учебного курса рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение курса «Информационная безопасность» отводится по 1 часу в неделю в 9 классе. Программа рассчитана на 34 учебных часа.

Характеристика личностных, метапредметных и предметных результатов освоения учебного курса

№	Название раздела (темы)	Планируемые результаты		
		личностные	предметные	метапредметные
1	Безопасность общения	<p><i>осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;</i></p> <p><i>освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;</i></p> <p><i>сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.</i></p>	<p>Выпускник научится:</p> <ul style="list-style-type: none"> - анализировать доменные имена компьютеров и адреса документов в интернете. <p>Выпускник овладеет:</p> <ul style="list-style-type: none"> - приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п. <p>Выпускник получит возможность овладеть:</p> <ul style="list-style-type: none"> - основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности; 	<p>Регулятивные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - идентифицировать собственные проблемы и определять главную проблему; - выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; <p>Познавательные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - выделять явление из общего ряда других явлений; - определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений; - строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; <p>Коммуникативные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - строить позитивные отношения в процессе учебной и познавательной деятельности; - критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;

				- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
2	Безопасность устройств	готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;	<p>Выпускник научится:</p> <ul style="list-style-type: none"> - безопасно использовать средства коммуникации; <p>Выпускник овладеет:</p> <ul style="list-style-type: none"> - приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п. <p>Выпускник получит возможность овладеть:</p> <ul style="list-style-type: none"> - использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных. 	<p>Регулятивные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - ставить цель деятельности на основе определенной проблемы и существующих возможностей; - выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; <p>Познавательные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - излагать полученную информацию, интерпретируя ее в контексте решаемой задачи; - самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; <p>Коммуникативные универсальные учебные действия.</p> <p>В результате освоения учебного курса</p> <ul style="list-style-type: none"> - делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его. - целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
3	Безопасность	- освоенность социальных	Выпускник научится:	Регулятивные универсальные учебные действия.

	<p>информации</p>	<p><i>норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;</i></p> <p><i>- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.</i></p>	<p>- безопасно вести и применять способы самозащиты при попытке мошенничества, - безопасно использовать ресурсы интернета.</p> <p>Выпускник овладеет:</p> <p>- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.</p> <p>Выпускник получит возможность овладеть: основами соблюдения норм информационной этики и права;</p>	<p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> - составлять план решения проблемы (выполнения проекта, проведения исследования); - описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса; оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; <p>Познавательные универсальные учебные действия.</p> <p>В результате освоения учебного курса обучающийся сможет:</p> <ul style="list-style-type: none"> – критически оценивать содержание и форму текста; – определять необходимые ключевые поисковые слова и запросы. <p>Коммуникативные универсальные учебные действия.</p> <p>В результате освоения учебного курса</p> <ul style="list-style-type: none"> -выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; - использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов).
--	--------------------------	--	--	--

Содержание программы учебного курса.

Содержание программы учебного курса соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

Тема раздела	Основное содержание по темам	Форма организации учебных занятий
Раздел №1 Безопасность общения		
Тема 1. Общение в социальных сетях и мессенджерах. 1 час.	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Урок-лекция Презентация к уроку
Тема 2. С кем безопасно общаться в интернете. 1 час.	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Урок-лекция Презентация к уроку
Тема 3. Пароли для аккаунтов социальных сетей. 1 час.	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Урок-лекция Презентация к уроку
Тема 4. Безопасный вход в аккаунты. 1 час.	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Урок-лекция Презентация к уроку
Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в	Урок-лекция Практическая работа

	мессенджерах.	
Тема 6. Публикация информации в социальных сетях. 1 час.	Персональные данные. Публикация личной информации.	Урок-лекция Презентация к уроку
Тема 7. Кибербуллинг. 1 час.	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Урок-лекция Презентация к уроку
Тема 8. Публичные аккаунты. 1 час.	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Урок-лекция Практическая работа
Тема 9. Фишинг. 2 часа.	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Урок-лекция Презентация к уроку
Выполнение и защита индивидуальных и групповых проектов. 3 часа.	Создание буклета и (или) презентации на тему «Безопасное общение в сети Интернет»	Самостоятельная работа на ПК Самостоятельная работа в сети Интернет
Раздел №2. Безопасность устройств.		
Тема 1. Что такое вредоносный код. 1 час.	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Урок-лекция Презентация к уроку
Тема 2. Распространение вредоносного кода. 1 час.	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	Урок-лекция Презентация к уроку
Тема 3. Методы защиты от вредоносных программ. 2 часа	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Урок-лекция Презентация к уроку
Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Урок-лекция Презентация к уроку

Выполнение и защита индивидуальных и групповых проектов. 3 часа.	Создание буклета и (или) презентации на тему «Защита персональных данных при использовании мобильных устройств»	Самостоятельная работа на ПК Самостоятельная работа в сети Интернет
Раздел №3 Безопасность информации.		
Тема 1. Социальная инженерия: распознать и избежать. 1 час.	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Урок-лекция Презентация к уроку
Тема 2. Ложная информация в Интернете. 1 час.	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Урок-лекция Групповая работа в сети Интернет
Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Урок-лекция Презентация к уроку
Тема 4. Беспроводная технология связи. 1 час.	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Урок-лекция Презентация к уроку
Тема 5. Резервное копирование данных. 1 час.	Безопасность личной информации. Создание резервных копий на различных устройствах.	Урок-лекция Создание резервных копий на мобильных устройствах
Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Урок-лекция Презентация к уроку
Выполнение и защита индивидуальных и групповых проектов. 3 часа.	Создание буклета и (или) презентации на тему «Правила безопасности при виртуальных контактах»	Самостоятельная работа на ПК Самостоятельная работа в сети Интернет
Повторение. Волонтерская практика. 3 часа.		

Календарно - тематическое планирование учебного курса

№	тема	количество часов	основное содержание	Характеристика основных видов учебной деятельности обучающихся	дата
Раздел 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах.	1	Социальная сеть. История социальных сетей. Мессенджеры.. Назначение социальных сетей и мессенджеров. . Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.	
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями установками коллектива, общества в целом. Изучает правила сетевого общения.	
3	Пароли для аккаунтов в социальных сетях	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применять.	
4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.	
5	Настройка конфиденциальности в социальных сетях.	1	Настрой ка приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.	
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.	
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознаёт провокации и попытки манипуляции со стороны виртуальных собеседников.	

8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.	
9	Фишинг	2	Фишинг как мошеннический приём. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни или жизни знакомых. Разработка и распространение памятки по противодействию фишингу.	
10	Выполнение и защита индивидуальных и групповых проектов	3	Создание буклета и (или) презентации на тему «Безопасное общение в сети Интернет»	Самостоятельная работа. Работа в группах.	
Раздел 2. «Безопасность устройств»					
11	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.	
12	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.	
13	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки.	
14	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.	
15	Выполнение и защита индивидуальных и групповых проектов	3	Создание буклета и (или) презентации на тему «Защита персональных данных при использовании мобильных устройств»	Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство	

				(аргументы), факты; гипотезы, аксиомы, теории.	
Раздел 3 «Безопасность информации»					
16	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.	
17	Ложная информация в Интернете	1	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам.	
18	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.	
19	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	
20	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.	
21	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.	
22	Выполнение и защита индивидуальных и групповых проектов	3		Создание буклета и (или) презентации на тему «Правила безопасности при виртуальных контактах»	
23	Повторение, волонтерская	3		Проведение мероприятий по сетевой	

	практика, резерв			безопасности с учащимися ОУ.	
	ИТОГО	34			