МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КАМЧАТСКОГО КРАЯ

ПРИКАЗ № 338

г. Петропавловск-Камчатский 21.04.2009 года

Об использовании сети Интернет в образовательных учреждениях

В связи с выполнением мероприятий по подключению общеобразовательных учреждений Корякского округа Камчатского края к сети Интернет, а так же в целях упорядочения условий и порядка использования сети Интернет

ПРИКАЗЫВАЮ:

1. Утвердить:

Типовые правила использования сети Интернет в общеобразовательном учреждении (приложение № 1).

Типовой регламент по работе учителей и школьников в сети Интернет (приложение № 2).

Типовую инструкцию для сотрудников общеобразовательных учреждений о порядке действий при осуществлении контроля за использованием учащимися сети Интернет (приложение № 3).

Примерную инструкцию пользователя по компьютерной безопасности (приложение № 4).

Регламент работы по защите и обновлению антивирусного программного обеспечения (приложение № 5).

Примерное положение о Совете образовательного учреждения по вопросам регламентации доступа к информации в Интернете (приложение № 6).

2. Руководителям государственных и муниципальных образовательных учреждений:

На основании типовых инструкций и регламентов разработать и утвердить правила и регламент использования учащимися сети Интернет, должностные инструкции для лиц, обеспечивающих работу учащихся в сети Интернет и контроль за использованием сети Интернет в образовательном учреждении, обеспечению мер компьютерной безопасности.

Назначить ответственных лиц за координацию работы в образовательном учреждении по использованию сети Интернет и осуществлению контроля за ее использованием.

Для исключения доступа к ресурсам сети Интернет, не совместимыми с задачами образования установить на все компьютеры, имеющие выход в Интернет программу СКФ, входящую в пакет лицензионного программного обеспечения «Первая помощь».

3. Органам управления образованием муниципальных образований в Корякском округе Камчатского края обеспечить выполнение необходимых мероприятий по упорядочению использования сети Интернет в подведомственных образовательных учреждениях.

4. Контроль за исполнением настоящего приказа возложить на заместителя Министра Н.Г. Розгачеву

Министр В.Л. Тюменцев

Исп.
Розгачева Наталья Геннадьвна
(415-2) 42-47-07

Приложение № 1 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

ТИПОВЫЕ ПРАВИЛА ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

I. Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет через ресурсы общеобразовательного учреждения (далее – Образовательное учреждение) учащимися, преподавателями и сотрудниками Образовательного учреждения.

1.2. Настоящие Правила имеют статус локального нормативного акта Образовательного учреждения. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства Российской Федерации.

1.3. Использование сети Интернет в Образовательном учреждении подчинено следующим принципам:

- соответствия образовательным целям;
- способствования гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

II. Организация и политика использования сети Интернет в общеобразовательном учреждении

2.1. Использование сети Интернет в Образовательном учреждении возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в Образовательном учреждении, с настоящими Правилами.

Ознакомление и согласие удостоверяется подписью лица в Листе ознакомления и согласия с Правилами. Ознакомление и согласие несовершеннолетнего удостоверяется, помимо его подписи, также подписью его родителя или иного законного представителя.

2.2. Руководитель образовательного учреждения (Директор Образовательного учреждения) является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет в Образовательном учреждении, а также за внедрение соответствующих технических, правовых и др. механизмов в Образовательном учреждении.

2.3. Непосредственное определение политики доступа в Интернет осуществляет Общественный Совет Образовательного учреждения, состоящий из представителей педагогического коллектива, сотрудников Образовательного учреждения, родительского комитета и ученического самоуправления.

Общественный Совет Образовательного учреждения:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, запрещенную законодательством Российской Федерации и/или несовместимую с задачами образовательного процесса с учетом социокультурных особенностей Камчатского края;

- определяет характер и объем информации, публикуемой на Интернет-ресурсах Образовательного учреждения;

2.4. Во время занятий контроль за использованием учащимися сети Интернет в соответствии с настоящим Правилами осуществляет преподаватель, ведущий занятие.

Преподаватель:

- наблюдает за использованием компьютера и сети Интернет учащимися;

- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;

- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

Во время использования сети Интернет для свободной работы контроль за использованием сети Интернет осуществляет ответственное лицо, назначенное директором образовательного учреждения.

Ответственное лицо:

- определяет время и место для свободной работы в сети Интернет учащихся, преподавателей и сотрудников Образовательного учреждения с учетом использования соответствующих технических мощностей Образовательного учреждения в образовательном процессе, а также длительность сеанса работы одного человека;

- контролирует объем трафика Образовательного учреждения в сети Интернет;

- наблюдает за использованием компьютера и сети Интернет учащимися;

- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;

- не допускает учащегося к работе в Интернете в предусмотренных настоящими Правилами случаях;

- принимает предусмотренные настоящими Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

2.5. При использовании сети Интернет в Образовательном учреждении осуществляется доступ только на ресурсы, содержание которых не противоречит законодательству Российской Федерации и не является несовместимым с целями и задачами образования и воспитания учащихся.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контекстного ограничения доступа, установленного в Образовательном учреждении или предоставленного оператором услуг связи.

Использование сети Интернет в Образовательном учреждении без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только для лиц, достигших 18 лет, с индивидуального разрешения Директора Образовательного учреждения.

Пользователи сети Интернет в Образовательном учреждении понимают, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет в связи с частотой обновления ресурсов сети Интернет и в связи с этим осознают возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству Российской Федерации и является несовместимым с целями и задачами образовательного процесса. Участники процесса использования сети Интернет в Образовательном учреждении осознают, что Образовательное учреждение не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах Образовательного учреждения.

2.6. Принятие решения о политике доступа к ресурсам/группам ресурсов сети Интернет принимается Общественным Советом Образовательного учреждения самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

- преподаватели Образовательного учреждения и других образовательных учреждений;
- лица, имеющие специальные знания либо опыт работы в рассматриваемой области;
- представители органов управления образованием.

При принятии решения Общественный Совет Образовательного учреждения, эксперты руководствуются:

- законодательством Российской Федерации;
- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;
- интересами учащихся, целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.7. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, осуществляется лицом, назначенным Директором Образовательного учреждения. Категории ресурсов, в

соответствии с которыми определяется политика использования сети Интернет в Образовательном учреждении и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.8. Принципами размещения информации на Интернет-ресурсах Образовательного учреждения являются:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защита персональных данных учащихся, преподавателей и сотрудников;
- достоверность и корректность информации.

Персональные данные об учащихся (фамилия и имя, класс, возраст, фотография, место жительства, телефоны и иные контакты, иные сведения личного характера) могут размещаться на Интернет-ресурсах Образовательного учреждения (сайт Образовательного учреждения и ее подразделений) только с письменного согласия родителей или иных законных представителей учащихся. Персональные данные преподавателей и сотрудников Образовательного учреждения размещаются на Интернет-ресурсах Образовательного учреждения только с письменного согласия преподавателя или сотрудника, чьи персональные данные размещаются.

В информационных сообщениях о мероприятиях на сайте Образовательного учреждения и ее подразделений без согласия лица или его законного представителя могут быть упомянуты только фамилия и имя учащегося либо фамилия, имя и отчество преподавателя\сотрудника\родителя.

При истребовании такого согласия представитель Образовательного учреждения разъясняет лицу возможные риски и последствия опубликования персональных данных. Образовательное учреждение не несет ответственности в случае наступления таких последствий, если имелось письменное согласие лица (его представителя) на опубликование персональных данных.

III. Процедура использования сети Интернет

3.1. Использование сети Интернет в Образовательном учреждении осуществляется, как правило, в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. По разрешению ответственного лица учащиеся (с согласия родителей, законных представителей), преподаватели и сотрудники вправе:

- размещать собственную информацию в сети Интернет на Интернет-ресурсах Образовательного учреждения;
- иметь учетную запись электронной почты на Интернет-ресурсах Образовательного учреждения.

3.3. Учащемуся запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство

Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер Образовательного учреждения без разрешения ответственного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. Ответственное лицо проверяет, является ли данный учащийся допущенным до самостоятельной работы в сети Интернет.

3.5. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе ответственному лицу с указанием его Интернет-адреса (URL) и покинуть данный ресурс.

Ответственное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения директора образовательного учреждения для оценки ресурса и принятия решения по политике доступа к нему в соответствии с п.2.3 настоящих Правил;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);
- если обнаруженный ресурс явно нарушает законодательство Российской Федерации – сообщить об обнаруженном ресурсе по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- Интернет-адрес (URL) ресурса;
- Тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательного процесса;
- Дату и время обнаружения;
- Информацию об установленных в Образовательном учреждении технических средствах технического ограничения доступа к информации.

Приложение № 2 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

ТИПОВОЙ РЕГЛАМЕНТ ПО РАБОТЕ УЧИТЕЛЕЙ И ШКОЛЬНИКОВ В СЕТИ ИНТЕРНЕТ

I. Общие положения

«Точка доступа» к сети Интернет предназначена для обслуживания учителей и учеников школы. Сотрудники и учащиеся школы допускаются к работе на бесплатной основе**.**

К работе в Интернет допускаются пользователи, прошедшие предварительную регистрацию у администратора школьной локальной вычислительной сети.

Выход в Интернет осуществляется с 8^{00} до 19^{00} (кроме воскресенья). Последняя пятница месяца – день профилактики.

Предоставление сеанса работы в Интернет осуществляется, как правило через прокси-сервер, на основании предварительной записи в журнале администратора школьной локальной вычислительной сети или при наличии свободных мест в зависимости от категории пользователя:

- учащимся предоставляется доступ в компьютерных классах или на отдельных рабочих местах согласно расписанию занятий (график работы компьютерных классов составляется на основании ежемесячно подаваемых служебных записок на имя заместителя директора по ИКТ (заместителя директора по учебно – воспитательной работе) с приложением расписания занятий и учебных планов);
- учителям предоставляется доступ согласно ежемесячно подаваемым служебным запискам на имя заместителя директора по ИКТ (заместителя директора по учебно – воспитательной работе) при этом учителю выдается регистрационное имя, пароль и график работы (не менее 2 часов в неделю). Этот ресурс может делиться на кванты времени, равные не менее 30 минутам;
- остальным пользователям предоставляется доступ при наличии резерва пропускной способности канала передачи.

Для работы в Интернет необходимо иметь при себе документ, удостоверяющий личность пользователя (пропуск учащегося, пропуск учителя или регистрационные карточки с логином и паролем).

По всем вопросам, связанным с доступом в Интернет, следует обращаться к администратору школьной локальной вычислительной сети.

II. Правила работы

При входе в класс, необходимо обратиться к администратору за разрешением для работы. При наличии свободных мест, после регистрации в журнале учета, посетителю предоставляется рабочая станция. Для доступа в Интернет и использования электронной почты установлен программный продукт "Internet Explorer", «Outlook Express». Отправка электронной почты с присоединенной к письму информацией, запись информации на дискеты и CD-диски осуществляется у администратора. Дополнительно установлено программное обеспечение: текстовые редакторы семейства "Microsoft Office".

1. Пользователь обязан выполнять все требования администратора.
2. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации (логин) и пароль.
3. За одним рабочим местом должно находиться не более одного пользователя.
4. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.
5. Каждому пользователю, при наличии технической возможности, предоставляется персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.
6. Пользователю разрешается записывать полученную информацию на личные дискеты. Дискеты должны предварительно проверяться на наличие вирусов. Запрещается любое копирование с дискет на жесткие диски.
7. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции.
8. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.
9. Запрещена передача информации, представляющую коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.
10. Запрещается работать с объемными ресурсами (video, audio, chat, игры и др.) без согласования с администратором.

11. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
12. Пользователь обязан сохранять оборудование в целости и сохранности.
13. Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить системному администратору.

При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния пользователь получает первое предупреждение и лишается права выхода в Интернет сроком на 1 месяц. При повторном административном нарушении – пользователь лишается доступа в Интернет.

При возникновении технических проблем пользователь обязан поставить в известность администратора школьной локальной вычислительной сети.

III. Правила регистрации

Для доступа в Интернет пользователей необходимо пройти процесс регистрации.

1. Регистрационные логин и пароль учащиеся получают у заместителя директора по ИКТ (заместителя директора по учебно – воспитательной работе), учителя информатики через своего классного руководителя.
2. Регистрационные логин и пароль учителя получают у заместителя директора по ИКТ(заместителя директора по учебно – воспитательной работе) при предъявлении удостоверения личности и письменного заявления.
3. После ввода сетевого имени и пароля пользователь получает либо сообщение об ошибке (тогда ее необходимо исправить) либо доступ.
4. Перед работой необходимо ознакомиться с "Памяткой" и расписаться в журнале учета работы в Интернет, который хранится у администратора.

IV. Памятка по использованию ресурсов сети Интернет

1. Пользователь обязан выполнять все требования администратора локальной сети.
2. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации и пароль. После окончания работы необходимо завершить свой сеанс работы, вызвав в меню «Пуск» команду «Завершение сеанса <имя>» либо в меню «Пуск» команду «Завершение работы» и «Войти в систему под другим именем».
3. За одним рабочим местом должно находиться не более одного пользователя.

4. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.
5. Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.
6. Пользователю разрешается переписывать полученную информацию на личные дискеты. Дискеты предварительно проверяются на наличие вирусов.
7. Разрешается использовать оборудование классов только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих целях запрещено.
8. Запрещена передача внешним пользователям информации, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайне, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.
9. Запрещается работать с объемными ресурсами (video, audio, chat, игры) без согласования с администратором.
10. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
11. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции. Запрещается перегружать компьютер без согласования с администратором локальной сети.
12. Пользователь обязан сохранять оборудование в целости и сохранности.

При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. В случае нарушения правил работы пользователь лишается доступа в сеть. За административное нарушение, не влекущее за собой порчу имущества, вывод оборудования из рабочего состояния и не противоречащие принятым правилам работы пользователь получает первое предупреждение. При повторном административном нарушении - пользователь лишается доступа в Интернет без права восстановления.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

Приложение № 3 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

ТИПОВАЯ ИНСТРУКЦИЯ ДЛЯ СОТРУДНИКОВ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ О ПОРЯДКЕ ДЕЙСТВИЙ ПРИ ОСУЩЕСТВЛЕНИИ КОНТРОЛЯ ЗА ИСПОЛЬЗОВАНИЕМ УЧАЩИМИСЯ СЕТИ ИНТЕРНЕТ

1. Настоящая Инструкция устанавливает порядок действий при обнаружении сотрудниками образовательных учреждений:

1) возможности доступа учащихся к потенциально опасному контенту;

2) вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для учащихся, доступ к которому не противоречит принятым нормативным актам на федеральном и региональном уровнях, муниципальном уровне, а также на уровне образовательного учреждения.

2. Контроль за использованием учащимися сети Интернет осуществляют:

1) во время проведения занятий – преподаватель, проводящий занятие и (или) специально уполномоченное руководителем образовательного учреждения на осуществление такого контроля лицо;

2) во время использования сети Интернет для свободной работы учащихся - лицо, назначенное руководителем образовательного учреждения на осуществление такого контроля.

3. Лицо, осуществляющее контроль за использованием учащимися сети Интернет:

- определяет время и место работы учащихся в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного учащегося;
- способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;
- наблюдает за использованием компьютеров и сети Интернет учащимися;
- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся порядка использования сети Интернет и предъявляемых к учащимся требований при работе в сети Интернет;
- не допускает учащегося к работе в Интернете в предусмотренных Правилами использования сети Интернет случаях;
- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу /группе ресурсов/, несовместимых с задачами образования.

4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием учащимися сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством

Российской Федерации или иному потенциально опасному для учащихся контенту, ответственное лицо направляет соответствующую информацию руководителю образовательного учреждения, который принимает необходимое решение.

5. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для учащихся, доступ к которому не противоречит принятым нормативным актам на федеральном и региональном уровнях, муниципальном уровне, а также на уровне образовательного учреждения.

Приложение № 4 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

ПРИМЕРНАЯ ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Для обеспечения безопасной работы в Интернет, ответственный специалист в общеобразовательном учреждении за обеспечение работы в сети Интернет должен выполнить следующее:

1. Установить последние обновления операционной системы Windows (http://windowsupdate.microsoft.com)
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
3. Скачать с сайта www.microsoft.com программное обеспечение Windows Defender и установить на все компьютеры. Включить режим автоматической проверки. Включить режим проверки по расписанию каждый день.
4. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
5. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
6. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
   a. Режим автоматической защиты должен быть включен постоянно
   b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
   c. Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
7. Не реже одного раза в месяц посещать сайт http://windowsupdate.microsoft.com и проверять установлены ли последние обновления операционной системы.
8. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
9. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.

10. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.

11. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

Приложение № 5 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

РЕГЛАМЕНТЫ РАБОТЫ ПО ЗАПУСКУ И ОБНОВЛЕНИЮ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В качестве источника угроз информационной безопасности может выступать человек либо группа людей, а также некие, независящие от деятельности человека, проявления. Исходя из этого, все источники угроз можно разделить на три группы:

- **Человеческий фактор**. Данная группа угроз связана с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Угрозы этой группы можно разделить на:
  - *внешние*, к ним относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур.
  - *внутренние*, к ним относятся действия персонала компаний, а также пользователей домашних компьютеров. Действия данных людей могут быть как умышленными, так и случайными.
- **Технический фактор**. Эта группа угроз связана с техническими проблемами – физическое и моральное устаревание использующегося оборудования, некачественные программные и аппаратные средства обработки информации. Все это приводит к отказу оборудования и зачастую потери информации.
- **Стихийный фактор**. Эта группа угроз включает в себя природные катаклизмы, стихийные бедствия и прочие форс-мажорные обстоятельства, независящие от деятельности людей.

Все три источника угроз необходимо обязательно учитывать при разработке системы защиты информационной безопасности.

Развитие современных компьютерных технологий и средств связи дает возможность злоумышленникам использовать различные источники распространения угроз. Рассмотрим их подробнее:

Интернет

Глобальная сеть Интернет уникальна тем, что не является чьей-то собственностью и не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией. Сейчас любой человек может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб-ресурс.

Однако эти же особенности глобальной сети предоставляют злоумышленникам возможность совершения преступлений в Интернете, при этом затрудняя их обнаружение и наказание.

Злоумышленники размещают вирусы и другие вредоносные программы на веб-ресурсах, "маскируют" их под полезное и бесплатное программное обеспечение. Кроме того, скрипты, автоматически запускаемые при открытии веб-страницы, могут выполнять вредоносные действия на вашем компьютере, включая изменение системного реестра, кражу личных данных и установку вредоносного программного обеспечения.

Используя сетевые технологии, злоумышленники реализуют атаки на удаленные частные компьютеры и сервера компаний. Результатом таких атак может являться выведение ресурса из строя, получение полного доступа к ресурсу, а, следовательно, к информации, хранящемся на нем, использование ресурса как части зомби-сети.

В связи с появлением кредитных карт, электронных денег и возможностью их использования через Интернет (интернет-магазины, аукционы, персональные страницы банков и т.д.) интернет-мошенничество стало одним из наиболее распространенных преступлений.

Интранет

Интранет – это внутренняя сеть, специально разработанная для управления информацией внутри компании или, например, частной домашней сети. Интранет является единым пространством для хранения, обмена и доступа к информации для всех компьютеров сети. Поэтому, если какой-либо из компьютеров сети заражен, остальные компьютеры подвергаются огромному риску заражения. Во избежание возникновения таких ситуаций необходимо защищать не только периметр сети, но и каждый отдельный компьютер.

Электронная почта

Наличие почтовых приложений практически на каждом компьютере, а также то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых жертв, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысячам своих абонентов.

Помимо угрозы проникновения вредоносных программ существуют проблема внешней нежелательной почты рекламного характера (спама). Не являясь источником прямой угрозы, нежелательная корреспонденция увеличивает нагрузку на почтовые сервера, создает дополнительный трафик, засоряет почтовый ящик пользователя, ведет к потере рабочего времени и тем самым наносит значительный финансовый урон.

Также важно отметить, что злоумышленники стали использовать так называемые спамерские технологии массового распространения и методы социального инжиниринга, чтобы заставить пользователя открыть письмо, перейти по ссылке из письма на некий интернет-ресурс и т.п. Из этого следует, что возможности фильтрации спама важны не только сами по себе, но и для противодействия некоторым новым видам интернет-мошенничества (например, фишингу), а также распространению вредоносных программ.

Съемные носители информации

Съемные носители – дискеты, CD-диски, флеш-карты – широко используются для хранения и передачи информации.

При запуске файла, содержащего вредоносный код, со съемного носителя вы можете повредить данные, хранящиеся на вашем компьютере, а также распространить вирус на другие диски компьютера или компьютеры сети.

Виды угроз.

Черви (Worms)

Данная категория вредоносных программ для распространения использует в основном уязвимости операционных систем. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому многие черви обладают достаточно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Вирусы (Viruses)

Программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – *заражение*.

Троянские программы (Trojans)

Программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Программы-рекламы (Adware)

Программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Программы-шпионы (Spyware)

Программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; в этом случает чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Потенциально опасные приложения (Riskware)

Программное обеспечение, которое не имеет какой-либо вредоносной функции, но может быть использовано злоумышленниками в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и ошибки. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся, например, некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, IRC-клиенты, FTP-сервера, всевозможные утилиты для остановки процессов или скрытия их работы.

Еще одним видом вредоносных программ, являющимся пограничным для таких программ как Adware, Spyware и Riskware, являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик.

Программы-шутки (Jokes)

Программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен,

либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Программы-маскировщики (Rootkit)

Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Программы-маскировщики модифицируют операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы

Программы, созданные для организации DoS-атак на удаленные сервера, взлома других компьютеров, а также являющиеся частью среды разработки вредоносного программного обеспечения. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов, сканеры уязвимостей, программы для взлома паролей, прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Хакерские атаки

Хакерские атаки – это действия злоумышленников или вредоносных программ, направленные на захват информационных данных удаленного компьютера, выведение системы из строя или получение полного контроля над ресурсами компьютера.

Некоторые виды интернет-мошенничества

Фишинг (Phishing) – вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера. Фишинг-сообщения составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, специально подготовленный злоумышленниками и являющийся копией сайта организации, от якобы имени которой пришло письмо. На данном сайте пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Дозвон на платные интернет-ресурсы – вид интернет-мошенничества, связанный с несанкционированным использованием платных интернет-ресурсов (чаще всего это веб-сайты порнографического содержания). Установленные злоумышленниками программы (dialers) инициируют модемное соединение с вашего компьютера на платный номер. Чаще всего используемые номера имеют очень высокие тарифы, в результате пользователь вынужден оплачивать огромные телефонные счета.

Навязчивая реклама

Навязчивая реклама – это всплывающие окна и рекламные баннеры, открывающиеся при работе с веб-сайтами. Как правило, информация, содержащаяся в них, не бывает полезной. Демонстрация всплывающих окон и баннеров отвлекает пользователя от основных задач, увеличивает объем трафика.

Спам (Spam)

Спам – это анонимная массовая рассылка нежелательных почтовых сообщений. Так, спамом являются рассылки рекламного, политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно увеличивает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Признаки заражения

Есть ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения либо воспроизводятся непредусмотренные звуковые сигналы;
- неожиданно открывается и закрывается лоток CD/DVD-ROM-устройства;
- произвольно, без вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Есть также косвенные признаки заражения вашего компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;

- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- веб-браузер (например, Microsoft Internet Explorer) "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении.

Что делать при наличии признаков заражения

Если вы заметили, что ваш компьютер "ведет себя подозрительно",

1. Отключите компьютер от интернета и локальной сети, если он к ней был подключен.
2. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows, который вы создавали при установке операционной системы на компьютер.
3. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флеш-карту и пр.).
4. Установите антивирусную программу, если вы этого еще не сделали.
5. Обновите сигнатуру угроз программы. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.
6. Запустите полную проверку компьютера

Профилактика заражения

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является своевременная *профилактика*. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит избегать вирусных атак.

Правило № 1: *защитите компьютер с помощью антивирусных программ и программ безопасной работы в интернете*. Для этого:

- Безотлагательно установите антивирусную программу.
- Регулярно обновляйте сигнатуры угроз, входящие в состав программы.

Правило № 2: *будьте осторожны при записи новых данных на компьютер*:

- Проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-карты и пр.) перед их использованием.
- Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми.
- Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
- Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью антивирусной программы.
- Внимательно относитесь к выбору посещаемых вами интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

Правило № 3: *пользуйтесь сервисом Windows Update* и регулярно устанавливайте обновления операционной системы Microsoft Windows.

Правило №4: *покупайте дистрибутивные копии программного обеспечения у официальных продавцов*.

Правило № 5: *ограничьте круг людей, допущенных к работе на вашем компьютере*.

Правило № 6: *уменьшите риск неприятных последствий возможного заражения*:

- Своевременно делайте резервное копирование данных.
- Создайте диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя "чистую" операционную систему.

Правило № 7: *регулярно просматривайте список установленных программ на вашем компьютере*. Для этого вы можете воспользоваться пунктом **Установка/удаление программ** в **Панели инструментов** или просто просмотреть содержимое каталога **Program Files**, каталога автозагрузки.

Основные антивирусные программы:

1. Kaspersky Antivirus – входит в пакет «Первая помощь»
2. Norton Antivirus
3. Dr. Web
4. NOD 32
5. Mc Afee
6. Panda Antivirus

Приложение №6 к приказу
Министерства образования и науки
Камчатского края
от 21.04.2009 г. № 338

ПРИМЕРНОЕ ПОЛОЖЕНИЕ О СОВЕТЕ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ПО ВОПРОСАМ РЕГЛАМЕНТАЦИИ ДОСТУПА К ИНФОРМАЦИИ В ИНТЕРНЕТЕ

1. В соответствии с настоящим Положением о Совете образовательного учреждения по вопросам регламентации доступа к информации в Интернете (далее – "Совет") целью создания Совета является принятие мер для исключения доступа учащихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания учащихся.

2. Совет осуществляет непосредственное определение политики доступа в Интернет.

3. Совет создается из представителей педагогического коллектива, родительского комитета и ученического самоуправления в согласованном указанными лицами порядке.

4. Очередные Собрания Совета проходят с периодичностью, установленной Советом.

5. Совет:

- принимает решения о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, несовместимую с задачами образовательного процесса с учетом социокультурных особенностей Камчатской области, с учетом мнения членов Совета, а также иных заинтересованных лиц, представивших свои предложения в Совет;

- определяет характер и объем информации, публикуемой на Интернет-ресурсах образовательного учреждения;

6. Во время занятий контроль за использованием учащимися сети Интернет осуществляет преподаватель. Во время использования сети Интернет для свободной работы учащихся контроль за использованием сети Интернет осуществляет лицо, назначенное директором образовательного учреждения (далее – "Ответственное лицо").

7. Ответственное лицо:

- определяет время и место для свободной работы учащихся в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного учащегося;

- способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;

- наблюдает за использованием компьютеров и сети Интернет учащимися;

- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся порядка использования сети Интернет и предъявляемых к учащимся требований при работе в сети Интернет;

- не допускает учащегося к работе в Интернете в предусмотренных настоящими Правилами случаях;

- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.

8. Принятие решений о политике доступа к ресурсам/группам ресурсов сети Интернет осуществляется Советом самостоятельно либо с привлечением внешних экспертов, в качестве которых могут привлекаться:

- преподаватели образовательного учреждения и других образовательных учреждений;

- лица, имеющие специальные знания либо опыт работы в соответствующих областях;

- представители органов управления образованием.

9. При принятии решения Совет и эксперты должны руководствоваться:

- законодательством Российской Федерации;

- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;

- интересами учащихся, целями образовательного процесса;

- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

10. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, осуществляется на основании решений Совета лицом, назначенным ответственным директором образовательного учреждения.

11. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в образовательном учреждении и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.