МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

УПРАВЛЕНИЕ РОСКОМНАДЗОРА ПО ПЕРМСКОМУ КРАЮ

Д.А. Алдарова, Е.М. Глушкова,
А.Д. Иванов, А.А. Юшков

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ ДЛЯ ШКОЛЬНИКОВ И РОДИТЕЛЕЙ

Учебное пособие

Пермь 2019

УДК 004.7
ББК 32.973.202
А25

Алдарова Д.А., Глушкова Е.М., Иванов А.Д., Юшков А.А.
А25 Компьютерная безопасность для школьников и родителей / Д.А. Алдарова, Е.М. Глушкова, А.Д. Иванов, А.А. Юшков; Перм. гос. нац. исслед. ун-т. – Пермь, 2019. – 79 с.

ISBN 978-5-7944-3251-0

Описаны основные задачи, связанные с обеспечением информационной безопасности, которые возникают у начинающих пользователей компьютеров; приводятся правила личной компьютерной гигиены при работе за компьютером, включая использование антивирусных программ, брандмауэра и т.д.

Издание предназначено для учащихся общеобразовательных школ и родителей учеников.

УДК 004.7
ББК 32.973.202

Рекомендовано Управлением Роскомнадзора по Пермскому краю

Печатается по решению методической комиссии механико-математического факультета Пермского государственного национального исследовательского университета

ISBN 978-5-7944-3251-0

Оглавление

Вместо предисловия

Предлагаемая вашему вниманию книга является одним из первых изданий в РФ по компьютерной безопасности, предназначенных школьникам и их родителям.

Идея написания книги родилась у студентов 4-го курса механико-математического факультета Пермского государственного национального исследовательского университета специальности «Компьютерная безопасность» после прослушивания лекций по теме «Теоретические основы компьютерной безопасности». Идею студентов о написании книги для школьников поддержало Управление Роскомнадзора по Пермскому краю. В результате представителем этой организации и студентами была написана эта небольшая книга.

В ней рассматривается широкий круг вопросов, начиная от программного «устройства» компьютеров до правил личной компьютерной гигиены, а поэтому издание может быть полезно школьникам разных классов: от начальных до старших. Например, увлекающиеся программированием старшеклассники, ознакомившись с книгой, смогут более осознанно выбрать свой будущий профессиональный путь, а младшие с помощью родителей лучше узнать современную вычислительную технику и правила борьбы с компьютерными угрозами.

Книга написана профессиональным и понятным для неподготовленного читателя языком. Но читать ее нужно, взяв в руки ручку и делая необходимые записи на бумаге.

Мы желаем вам, дорогие читатели, чтобы вы без особых затруднений освоили материал, который студенты отобрали для вас, и активно использовали полученные из книги знания в своей повседневной работе за компьютером.

Доктор технических наук, профессор Пермского государственного национального исследовательского университета
О.Г. Пенский

Глава 1

Компьютерные вирусы и средства защиты от них

Компьютерные вирусы и их типы

Компьютерные вирусы – это специальные вредоносные программы, которые создаются злоумышленниками для получения какой-либо выгоды. На наши компьютеры они могут попасть либо через носимые запоминающие устройства (флешки, оптические диски, внешние жесткие диски и пр.), либо через компьютерные сети (чаще всего, через сеть Интернет). Эти программы устанавливаются на компьютер без согласия пользователя и могут вызывать ряд негативных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных и файлов пользователей, удаление данных или даже воздействие на работу аппаратных средств компьютера. При помощи таких программ ведется кража личной информации, промышленный шпионаж (сбор, изучение и распространение информации о конкретной фирме фирмами-конкурентами с целью получения некой выгоды), организуется удаленный доступ к компьютеру за счет взлома системы безопасности, а иногда даже и вымогание денежных средств. Поскольку киберпреступники стремятся придумать новые способы проникновения в компьютеры пользователей, в интернете можно встретить огромное количество разнообразных вирусных программ, число которых увеличивается с каждым днем.

На сегодня существуют следующие типы вирусов:

- *Файловые вирусы* – вредоносные программы, которые могут заразить файлы на жестком диске, флешке или любом другом запоминающем устройстве. Они могут попасть на наш компьютер, когда мы загружаем зараженный файл из сети Интернет или копируем зараженный файл с другого компьютера на свою флешку, приносим эту флешку домой и подключаем к своему компьютеру. Как видим, эти вирусы требуют вмешательства человека, чтобы попасть к нему на компьютер.
- *Черви* – вредоносные программы, которые не требуют вмешательства человека для заражения его компьютера. Используя компьютерные сети (например, сеть Интернет), они попадают на наш компьютер и посылают свои копии на другие компьютеры зараженной сети. Злоумышленники могут использовать данный тип вируса, чтобы удалить файлы с компьютера жертвы, зашифровать их с целью получения выкупа за их расшифровку или просто вывести из строя операционную систему.
- *Рекламные программы* – программы, которые, попадая на компьютер, показывают нам всевозможную рекламу, хотим мы того или нет. В большинстве случаев такие программы являются относительно безвредными, т.к. кроме демонстрации рекламы и изучения истории посещения сайтов с целью выдачи пользователю рекламы, которая могла бы быть ему интересна, они не производят никаких вредных воздействий.

- *Троянские программы* – программы, которые маскируются под обычные безвредные файлы или программы. После попадания на компьютер могут некоторое время бездействовать, оставаясь незамеченными для антивирусных программ. После активизации они вносят изменения в работу компьютера, могут уничтожить файлы или зашифровать их, а также украсть пароли от электронной почты, электронных кошельков, интернет-магазинов и пр.
- *Шпионские программы* – программы, которые могут следить за действиями пользователя и пересылать данные сторонним лицам без его ведома. Такие программы отслеживают поведение пользователей без их согласия и собирают информацию (например, регистрируют нажатия клавиш на компьютере пользователя, отслеживают, какие сайты посещал пользователь), впоследствии передавая ее третьим лицам (киберпреступникам). Собранная информация хранится на сервере киберпреступника. Шпионские программы также могут изменять определенные параметры на компьютере пользователя или препятствовать сетевым соединениям. Некоторые из вирусов-шпионов по результатам анализа действий пользователя могут демонстрировать рекламу в браузере, которая будет ему интересна.
- *Программы-вымогатели* – программы, которые, попдая на компьютер, зашифровывают личные файлы пользователя и требуют выкуп за их расшифровку. Кроме того, они могут заблокировать загрузку опера-

ционной системы. Зачастую выдают свои действия за действия правоохранительных органов. При отказе платить выкуп данные программы удаляют зашифрованные файлы.

- *Руткиты* – программы, которые используются для удаленного управления компьютером. Данный тип вирусов крайне трудно обнаружить. С помощью руткитов злоумышленники могут украсть файлы с нашего компьютера, установить другие вредоносные программы или заблокировать работу операционной системы.
- *Боты* – программы, которые используют ресурсы нашего компьютера для выполнения каких-либо автоматизированных действий. Могут использоваться для рассылки спама, распространения других вирусов, организации DDos-атак (атаки на компьютерные системы путем одновременной отправки большого количества запросов с множества компьютеров с целью перегрузки атакуемой системы, вывода ее из строя), использования ресурсов процессора для майнинга криптовалют.

Источники:

Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы // Лаборатория Касперского. URL: https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs (дата обращения: 13.08.2018).

Виды компьютерных вирусов // WELCOM-COMP.RU. URL: http://welcom-comp.ru/antivir_pc/58-vidy-kompyuternyh-virusov.html (дата обращения: 13.08.2018).

Типы и виды компьютерных вирусов // NastroiSam.RU. URL: https://nastroisam.ru/vidyi-kompyuternyih-virusov/ (дата обращения: 13.08.2018).

Средства защиты от компьютерных вирусов

Для защиты информации от компьютерных вирусов используются *общие средства защиты информации*, *специализированные программные средства (антивирусы)*, а также предпринимаются *профилактические меры*, которые позволяют уменьшить вероятность заражения компьютера вирусом.

Общие средства защиты информации полезны не только для защиты от вирусов, но и для защиты информации от повреждения. К таким средствам относятся:

- резервное копирование информации (создание копий файлов и системных областей дисков на дополнительном запоминающем устройстве);
- разграничение доступа к информации (предупреждение несанкционированного использования информации, защита от изменений программ и данных вирусами, неправильно работающими программами или ошибочными действиями пользователей).

Общие средства защиты информации важны для защиты от вирусов, однако недостаточно использовать только их. Необходимо также применять *специализированные программные средства*. Такие средства можно разделить на несколько видов в зависимости от их назначения:

1) Программы-детекторы

Такие программы предназначены для нахождения файлов, зараженных одним или несколькими известными вирусами. Они проверяют, есть ли в файлах на указанном пользователем запоминающем устройстве определенная последовательность байтов (для каждого вируса она различна). Если какой-либо файл содержит такую комбинацию байтов, программа-детектор уведомляет об этом пользователя. Недостаток таких программ заключается в том, что они способны найти далеко не все вирусы, а только те, комбинация байтов которых известна детектору. Существуют также такие программы-детекторы, которые можно настроить на обнаружение новых типов вирусов. Для этого им необходимо указать комбинацию байтов, присущую определенному вирусу.

Таким образом, с помощью программы-детектора нельзя точно определить, является ли файл здоровым или же зараженным вирусом, ведь в файле может скрываться вирус, неизвестный детектору.

2) Программы-доктора

Такие программы предназначены для лечения зараженных вирусами файлов. Программы-доктора убирают

из зараженного файла тело вируса, т.е. возвращают его в исходное состояние. Файлы, которые не удалось вылечить, как правило, просто удаляются. Большинство программ-докторов могут лечить только от определенного набора вирусов, в связи с чем такие программы быстро устаревают. Некоторые программы-доктора могут обучаться обнаружению и лечению новых типов вирусов.

3) Программы-ревизоры

Такие программы используются для того, чтобы выявить, заражен файл вирусом или нет, а также для нахождения поврежденных файлов. Принцип работы программ-ревизоров заключается в следующем: сначала они запоминают исходное состояние программ и файлов (предполагается, что в этот момент файлы не заражены). Далее во время работы компьютера программы-ревизоры сравнивают текущее состояние программ и системных областей дисков с исходным, и если эти состояния различаются, то пользователю сообщается о возможном заражении файлов. Большинство программ-ревизоров умеют выявлять изменения, вызванные, например, обновлением программы, и не подают ложных тревог пользователю. Чтобы проверить, изменился ли файл, такие программы вычисляют сначала длину файла и сравнивают с исходной. Однако одной такой проверки бывает недостаточно. Существуют вирусы, которые вносят изменения в файлы таким образом, что длина зараженного файла при этом остается прежней. Поэтому дополнительно читается весь файл и вычисляется его контрольная сумма. Контрольная сумма (или хеш) – это

определенное значение, рассчитанное для файла по одному из известных алгоритмов (например, CRC32, MD5, SHA-1). Используется контрольная сумма для проверки подлинности файлов и проверки их целостности (например, при их загрузке из сети Интернет). Изменить файл таким образом, чтобы его контрольная сумма осталась прежней, практически невозможно.

4) Доктора-ревизоры

Эти программы не только обнаруживают изменения в файлах и системных областях дисков, но и при выявлении изменений возвращают их в исходное состояние. То есть доктора-ревизоры представляют собой некий гибрид программ-ревизоров и программ-докторов. Такие программы являются более эффективными, чем программы-доктора, т.к. при восстановлении (лечении) файлов они используют заранее сохраненную информацию о первоначальном состоянии файлов. Благодаря этому доктора-ревизоры способны лечить файлы и от новых вирусов, которые еще даже не были созданы на момент написания данных антивирусных программ.

5) Программы-фильтры

Многие вирусы для размножения и нанесения вреда способны перехватывать обращения пользователя к операционной системе. Программы-фильтры ловят (перехватывают) такие обращения вирусов, тем самым не давая им нанести вред, и сообщают о них пользователю, который, в свою очередь, может разрешить или запретить выполнение данной операции. Такие программы являются

резидентными, т.е. они находятся постоянно в оперативной памяти компьютера. Преимущество использования программ-фильтров заключается в том, что такие программы способны ловить (обнаруживать) вирусы еще на ранних стадиях, до того как вирусы успели внести изменения, размножиться или же что-то испортить.

Ни один тип рассмотренных выше антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому лучшей защитой от вирусов будет являться многоуровневая защита. Выполнять роль разведки в такой системе будут программы-детекторы, проверяющие новые файлы и программы на наличие заражения. Первыми о вирусной атаке смогут сообщить резидентные программы, что поможет предотвратить заражение файлов. Если вирус все же заразил файлы, то программы-ревизоры смогут это обнаружить, а программы-доктора восстановить данные, если не была создана резервная копия. Однако программы-доктора не всегда лечат правильно, в отличие от них доктора-ревизоры как обнаруживают нападение вируса, так и контролируют правильность лечения файла. Необходимо также средство разграничения доступа для защиты данных от вирусов или неверно работающих программ. При этом в резерве будут находиться копии важных данных и эталонные диски с продуктами, что позволит восстановить работу при повреждении файлов на жестком диске.

К основным *профилактическим мерам*, которые также способны предотвратить заражение файлов вирусами, относятся:

- избегание использования неизвестных программ, а также программ, загруженных не с официальных сайтов разработчиков, т.к. чаще всего вирусы распространяются вместе с ними;
- использование лицензионного программного обеспечения;
- использование общих и специализированных защитных средств при работе на компьютере в любой информационной среде, например, в сети Интернет;
- проверка на наличие вирусов файлов, скачанных из сети Интернет.

Если не предпринимать никаких мер для защиты от вирусов, то последствия заражения могут быть очень серьезными!

Таким образом, для защиты от вирусов при работе за компьютером рекомендуется:

1. Установить на компьютер антивирусную программу и своевременно обновлять ее вирусную базу.
2. Использовать лицензионное программное обеспечение.
3. Проверять программы, скачанные из интернета (особенно с неофициальных сайтов), на наличие вирусов (с помощью антивирусной программы).
4. Периодически проверять на наличие вирусов жесткие диски компьютера.

5. Делать архивные копии наиболее ценной информации на внешнем носителе.
6. Перед использованием информации с внешних носителей (например, с флешки) проверять ее на наличие вирусов с помощью антивирусной программы.

Источники:

Алексеев Е.Г., Богатырев С.Д. Информатика: учебник. Саранск: Морд. гос. ун-т, 2009.

Дорош Ю.А. Компьютерные вирусы // УссуриВики. [2013–2013]. Дата обновления: 29.11.2013. URL: http://wiki.uspi.ru/index.php/Компьютерные_вирусы (дата обращения: 21.08.2018).

Косарев В.П., Еремин Л.В., Машникова О.В. Компьютерные системы и сети: учеб. пособие. М.: Финансы и статистика, 2000.

Макарова Н.В. Информатика: Учебник. 3-е изд. М.: Финансы и статистика, 2009.

Антивирусные программы и утилиты. Антивирусные программы

Антивирусная программа – это специализированная программа, предназначенная для обнаружения компьютерных вирусов, а также вредоносных программ и восстановления зараженных (измененных) такими программами файлов, а также для профилактики – предотвращения заражения (изменения) файлов или операционной системы вредоносным кодом.

Антивирусные утилиты

Антивирусные утилиты – это программы, которые ищут и удаляют вирусы, а также другие вредоносные программы на более глубоком уровне, чем обычные антивирусные программы.

Главное отличие антивирусных утилит от антивирусных программ заключается в следующем: антивирусные утилиты не имеют обновления своих баз. Они не работают все время, как антивирусные программы, а также не требуют инсталляции в систему. Чтобы проверить свой компьютер через несколько дней после скачивания утилиты, необходимо будет заново скачать ее с обновленными вирусными базами.

Обзор антивирусных программ и утилит

В настоящее время существует большое количество антивирусных программ и утилит. Рассмотрим и сравним наиболее популярные антивирусные программы (см. табл. 1).

Таблица 1

Сравнение антивирусных программ и утилит

Название программы	Стоимость лицензионного продукта (на 1 год)	Язык интерфейса
Kaspersky Free	Бесплатно	Русский
Dr.Web Security Space	1290 руб. в год	Русский
Avast! Free Antivirus	Бесплатно	Русский
Microsoft Security Essentials	Бесплатно в составе Windows Vista/Windows 7	Русский
Avira Free Antivirus	Бесплатно	Русский
COMODO Antivirus	Бесплатно	Русский
McAfee Internet Security	1899 руб. в год	Русский
AVG AntiVirus Free	Бесплатно	Русский
ESET NOD32 Internet Security	1950 руб. в год	Русский

Продолжение табл. 1

Анти-спам	Сетевой экран (брандмауэр)	Веб антивирус	Почтовый антивирус	Файловый антивирус	Название программы
-	-	+	+	+	*Kaspersky Free*
+	+	+	+	+	*Dr.Web Security Space*
-	-	+	+	+	*Avast! Free Antivirus*
-	- (интеграция с брандмауэром)	+	+	+	*Microsoft Security Essentials*
-	+	-	-	+	*Avira Free Antivirus*
-	+	+	-	+	*COMODO Antivirus*
+	+	+	+	+	*McAfee Internet Security*
-	-	+	+	+	*AVG AntiVirus Free*
+	+	+	+	+	*ESET NOD32 Internet Security*

Окончание табл. 1

Название программы	Родительский контроль	Общая оценка
Kaspersky Free	-	7/10
Dr.Web Security Space	+	9/10
Avast! Free Antivirus	-	7/10
Microsoft Security Essentials	-	6/10
Avira Free Antivirus	-	7/10
COMODO Antivirus	-	6/10
McAfee Internet Security	+	9/10
AVG AntiVirus Free	-	7/10
ESET NOD32 Internet Security	+	8/10

Источники:

Язов Ю. К., Соловьев С. В. Защита информации в информационных системах от несанкционированного доступа. Пособие. Воронеж: Кварта, 2015.

Антивирусная программа // Википедия. [2005–2018]. Дата обновления: 04.08.2018. URL: https://ru.wikipedia.org/?oldid=94355415 (дата обращения: 16.08.2018).

Лаборатория Касперского. URL: https://www.kaspersky.ru/ (дата обращения: 18.08.2018).

Dr.WEB Антивирус. URL: https://www.drweb.ru/ (дата обращения: 18.08.2018).

Avast. URL: https://www.avast.ru/ (дата обращения: 18.08.2018).

Microsoft // URL: https://www.microsoft.com/ru-ru/ (дата обращения: 18.08.2018).

Avira. URL: https://www.avira.com/ru/index (дата обращения: 18.08.2018).

Comodo. URL: https://ru.comodo.com/ (дата обращения: 18.08.2018).

McAfee. URL: https://www.mcafee.com/consumer/ru-ru/store/m0/index.html (дата обращения: 18.08.2018).

AVG. URL: https://www.avg.com/ru-ru/homepage (дата обращения: 18.08.2018).

ESET. URL: https://www.esetnod32.ru/ (дата обращения: 18.08.2018).

Глава 2

Средства защиты информации операционных систем

Пользователи ОС. Идентификация и аутентификация пользователя

Основой безопасности операционной системы (ОС) являются пользователи системы. Пользователи ОС являются владельцами файлов, которые они создали, обладают правами доступа к системным файлам и файлам других пользователей, от их имени запускаются различные процессы. При регистрации нового пользователя в ОС ему присваивается собственный идентификатор. Идентификатор – это некоторый набор битов, уникальный для каждого нового пользователя. Кроме того, каждый пользователь ОС принадлежит одной или нескольким группам пользователей. Каждая группа пользователей также имеет собственный уникальный идентификатор. При входе зарегистрированного пользователя в ОС происходит идентификация пользователя – предоставление ОС идентификатора данного пользователя. Чтобы убедиться в том, что пользователь действительно тот, за кого он себя выдает, и предъявленный при входе в систему идентификатор действительно принадлежит ему, производится аутентификация пользователя. Аутентификация – это проверка подлинности пользователя. Она осуществляется путем запроса у пользователя какой-либо дополнительной информации, которой владеет исключительно данный пользователь. Чаще всего для аутентификации поль-

зователя используется пароль (как наиболее простой способ), но также могут использоваться отпечатки пальцев, голосовые команды (при наличии системы распознавания голоса), лицо пользователя (при наличии системы распознавания лиц), ключ-карты и пр.

Хранение паролей в ОС. Алгоритмы шифрования паролей в ОС. Безопасность пароля

Если для аутентификации пользователя используется пароль, то при входе в систему происходит сравнение введенного пользователем пароля и пароля, хранящегося в системе. Если они совпадают, система предполагает, что пользователь является тем, за кого себя выдает, – производится вход в систему. Все пароли хранятся в системе в зашифрованном виде. При аутентификации пользователя с использованием пароля введенный пользователем пароль сначала шифруется, а затем происходит его сравнение с паролем, сохраненным в системе. Алгоритм, с помощью которого шифруются пароли, зависит от семейства и версии ОС. Основное свойство применяемых алгоритмов – использование при шифровании математических функций (т.е. последовательности математических операций для преобразования исходных данных в зашифрованные), для которых максимально сложно (в идеале – невозможно) подобрать обратную функцию (т.е. найти и применить к зашифрованным данным ту же последовательность математических операций, но в обратном порядке, и получить исходные данные).

При задании пароля необходимо придумать такой пароль, который можно будет легко запомнить. При этом пароль должен быть достаточно сложным, чтобы его было бы максимально трудно угадать или подобрать. Пароль будет небезопасным, если он будет включать в себя общедоступную информацию о пользователе (например, ФИО, дата рождения, клички домашних животных), состоять только из некоторой убывающей или возрастающей последовательности цифр, являться последовательностью букв в алфавитном порядке или каким-либо часто употребляемым словом. По нашему мнению, достаточно безопасный пароль должен состоять из не менее чем 8 символов, содержать в себе заглавные и строчные буквы латинского алфавита и цифры.

Разграничение доступа к объектам ОС

После авторизации пользователя и его входа в систему пользователю предоставляются только те ресурсы ОС и разрешается выполнять только те операции над объектами ОС, которые предоставлены ему администратором ОС. Администратор ОС – это отдельный сотрудник организации, который отвечает за установку и настройку ОС на рабочих местах. Если же говорить о домашнем компьютере, то администратор ОС – это тот человек, который устанавливал и настраивал ОС. Это можете быть вы или кто-то из вашей семьи. Объекты ОС – это ресурсы компьютера. Ресурсы могут быть как физическими (процессор, сегменты памяти, внешние

устройства), так и программными (файлы, программы). Тип операций зависит от типов ресурсов. Например, для файлов это операции чтения, записи, изменения и выполнения.

Разграничение доступа к объектам ОС в системах Windows

В операционных системах семейства Windows после авторизации пользователя и его входа в систему ему присваивается маркер доступа, который содержит уникальный идентификатор пользователя. Все процессы, создаваемые пользователем, содержат маркер доступа данного пользователя. Каждый объект, в свою очередь, имеет дескриптор безопасности. Дескриптор безопасности содержит список идентификаторов пользователей, которым разрешено выполнение операций над данным объектом, с указанием типов разрешенных операций. При попытке проведения операции над объектом ОС происходит сравнение маркера доступа пользовательского процесса с идентификаторами в дескрипторе безопасности объекта, и на основании результата сравнения выполнение операции разрешается или запрещается.

Задать список прав доступа к объекту можно в оконном диалоге в окне свойств объекта во вкладке «Безопасность» (см. рис. 1).

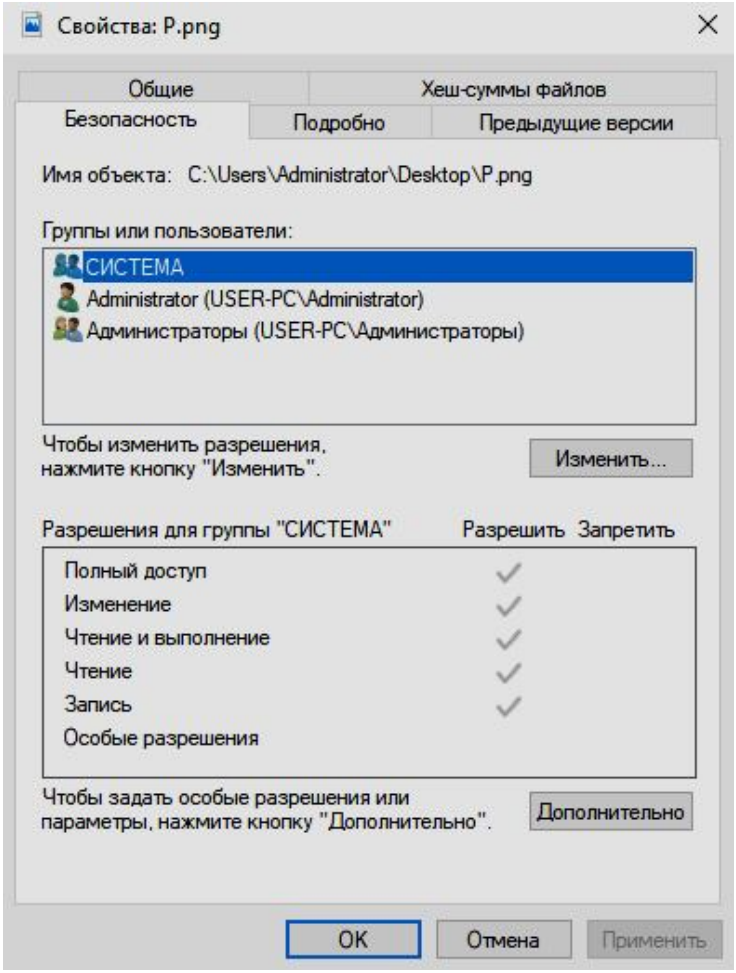


Рис. 1. Свойства объекта, вкладка «Безопасность»

Аудит

Помимо обеспечения разграничения доступа к объектам ОС система должна уметь отслеживать и записывать все происходящие события. Событиями называются любые действия пользователей и процессов, связанные с объектами ОС. Аудит – это процесс, позволяющий фиксировать в системном журнале все подобные действия. Аудит нужен для того, чтобы при возникновении сбоя в ОС или при обнаружении вирусной атаки на ОС была

возможность восстановить цепочку произошедших событий и найти причину сбоя или вирусный файл.

Аудит в системах Windows

В операционных системах семейства Windows инструментом аудита является утилита Event Viewer (Просмотр Событий). Утилита – это вспомогательная программа, предназначенная для упрощения работы с оборудованием компьютера или для упрощения настройки этого оборудования. Оборудование компьютера – это все компьютерные комплектующие, из которых он состоит (ЦП, ОП, материнская плата и пр.), и все внешние устройства, подключенные к компьютеру, исключая информацию, которая хранится или обрабатывается на компьютере. ОС записывает все события в три журнала – особых файла ОС, используемых для хранения событий:

- Системный журнал – содержит информационные сообщения, предупреждения и сообщения об ошибках, исходящих от компонентов операционной системы. Перечень регистрируемых в этом журнале событий определяется самой ОС и не может быть изменен пользователем.
- Журнал безопасности – содержит информационные сообщения об успешном или неудачном выполнении операций над объектами ОС. Перечень событий, регистрируемых в этом журнале, определяется системным администратором.

- Журнал приложений – содержит информационные сообщения, предупреждения и сообщения об ошибках, исходящих от приложений. Перечень регистрируемых в этом журнале событий определяется разработчиками приложений.

Каждая запись журнала содержит тип события, его дату и время, информацию о пользователе, который выполнил данное событие, код события и категорию задачи.

Брандмауэр

Брандмауэр – это программный (или программно-аппаратный) комплекс, защищающий компьютер от вредоносного трафика. Трафиком называется объем информации, передаваемой по сети за определенный временной промежуток. Он может измеряться как в пакетах, так и в битах (байтах, килобайтах, мегабайтах и т.д.). Пакет – это сформированный определенным образом блок данных, пересылаемый по сети. Каждый посылаемый и принимаемый пакет проходит через брандмауэр перед его отправкой в сеть или при сохранении на компьютере. На основе некоторого набора правил брандмауэр определяет, является этот пакет вредоносным или нет. Если является, то брандмауэр не пропускает такой пакет дальше. В системах семейства Windows существует встроенный брандмауэр. Брандмауэры зачастую входят также в состав антивирусных программ.

Все брандмауэры делятся на три типа:

- Пакетные фильтры.
- Сервера прикладного уровня.
- Сервера уровня соединения.

Все эти типы может включать в себя один брандмауэр.

Пакетные фильтры

Брандмауэры данного типа просматривают IP-адреса, флаги и номера TCP-портов (натуральное число, используемое для определения процесса-получателя пакета) и на основе этого принимают решение о пропуске или отбрасывании пакета. IP-адрес – это уникальный сетевой адрес устройства, позволяющий найти его другим устройствам сети, передать ему какую-либо информацию или получить информацию от него. Флаги – это биты, указывающие некоторые свойства пакета. Они имеют всего два значения: 1 – пакет обладает данным свойством, 2 – пакет данным свойством не обладает.

Для задания правил прохождения пакетов через пакетный фильтр используется таблица, записи которой содержат следующие поля:

- Действие.
- Тип пакета.
- Адрес источника.
- Порт источника.
- Адрес назначения.
- Порт назначения.
- Флаги.

Возможные действия – пропустить или отбросить пакет.

Тип пакета – TCP, UDP или ICMP.
Флаги – флаги из заголовка IP-пакета.

Сервера прикладного уровня

Брандмауэры данного типа используют сервера конкретных сервисов, которые пропускают через себя весь трафик, относящийся к данному сервису. Сервисы – это услуги, предоставляемые пользователю в сети. Между клиентом и местом назначения образуется дополнительное звено: клиент связан с брандмауэром, а брандмауэр – с местом назначения.

Список наиболее часто используемых сервисов:

- Поиск информации (WWW).
- Передача файлов(FTP).
- Электронная почта (SMTP, POP3).
- Управление удаленными компьютерами (Telnet, Rlogin).

Использование серверов прикладного уровня позволяет скрыть от внешней сети структуру локальной сети.

При задании правил доступа используются параметры:

- Имя пользователя.
- Название сервиса, к которому осуществляется доступ.
- Список компьютеров, с которых можно пользоваться данным сервисом.
- Временной промежуток, в который можно пользоваться данным сервисом, и др.

Сервера уровня соединения

Брандмауэр данного типа является транслятором TCP-соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего тот производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях, действуя как провод.

Источники:

Карпов В., Коньков К. Защитные механизмы операционных систем // Национальный Открытый Университет «ИНТУИТ». [2017–2017]. Дата обновления: 9.02.2017. URL: https://www.intuit.ru/studies/courses/2192/31/info (дата обращения: 23.08.2018).

Лясин Д.Н., Саньков С.Г. Методы и средства защиты компьютерной информации // Волжский Политехнический Институт (филиал ВолГТУ). URL: http://www.volpi.ru/umkd/zki/index.php?man=1 (дата обращения: 23.08.2018).

Брандмауэр // CIT Forum. URL: http://citforum.ru/security/internet/firewall.shtml (дата обращения: 29.08.2018).

Глава 3
Безопасность работы в сети Интернет

Протоколы сети Интернет

Передача данных в сети Интернет происходит по определенным правилам — *протоколам*. Они определяют команды и способ коммуникации (взаимодействия) между устройствами.

Передачу данных между устройствами описывает семиуровневая сетевая модель OSI (Open Systems Interconnect, в пер. с англ. «взаимодействие открытых систем»):

1. Уровень приложений (прикладной) – самый верхний уровень, представляет работу пользователя и приложений с сетью. Пользователи просто передают данные и не задумываются о том, как они будут передаваться.
2. Уровень представления – данные преобразуются в более низкоуровневый формат, чтобы быть такими, какими их ожидают получить программы.
3. Уровень сессии (сеансовый) – на этом уровне обрабатываются соединения между удаленными компьютерами, которые будут передавать данные.
4. Транспортный уровень – на этом уровне организуется надежная передача данных между компьютерами, а также проверка получения данных обоими устройствами (устройством-приемником и устройством-передатчиком).

5. Сетевой уровень – используется для управления маршрутизацией (определением маршрута следования) данных в сети, пока они не достигнут целевого узла (точки назначения). На этом уровне пакеты могут быть разбиты на более мелкие части, которые будут собраны получателем.
6. Уровень соединения (канальный, передачи данных) – отвечает за способ установки соединения между компьютерами и поддержания его надежности с помощью существующих физических устройств и оборудования.
7. Физический уровень – отвечает за обработку данных физическими устройствами, включает в себя программное обеспечение, которое управляет соединением на физическом уровне, например, Ethernet или Wi-Fi.

В этой модели физический уровень – нижний, каждый следующий уровень вплоть до верхнего уровня приложения строится на основе предыдущего и обеспечивается его средствами. Поэтому можно сказать, что при отправке данные последовательно проходят все семь уровней до нижнего, пересылаются, а на другом компьютере снова преобразуются до уровня приложений.

Для простоты далее будем рассматривать упрощенную модель TCP/IP (рис. 2):

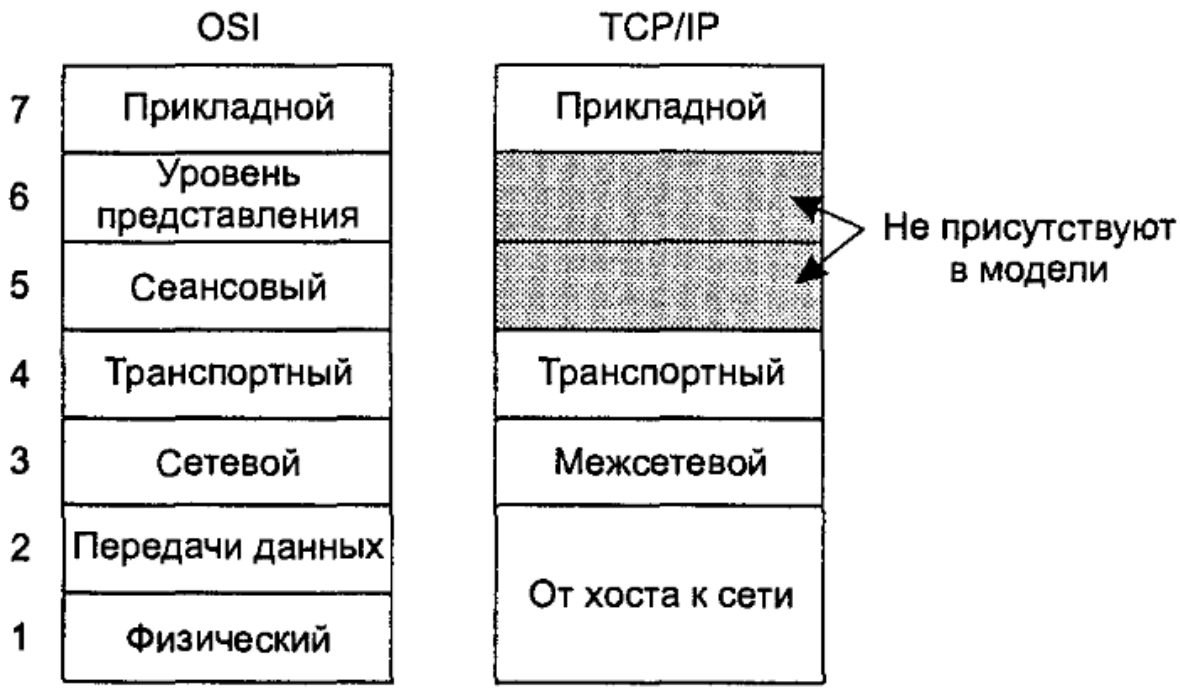


Рис. 2. Упрощенная модель TCP/IP

В данной модели физический и уровень передачи данных объединены в уровень «от хоста к сети» (англ. host-to-network), а сеансового и уровня представления просто нет, ведь как показала практика, большинство приложений в них мало нуждается.

Для каждого уровня существует свой набор протоколов. Для уровня передачи данных это протокол MAC (Media Access Control, в пер. с англ. «управление доступом к среде»). У каждого устройства, подключенного к сети, есть уникальный MAC-адрес, заданный производителем. По этому адресу любое устройство можно однозначно определить. MAC-адрес называют физическим адресом устройства. Только зная MAC-адрес

нужного устройства, маршрутизатор сможет начать пересылку пакетов данных, иначе данные не будут отправлены. Для того чтобы посмотреть физический адрес сетевой карты вашего устройства под управлением ОС Windows, введите в командной строке команду ipconfig – all. Вы увидите список настроенных подключений и параметры каждого из них, в том числе физический адрес вашего устройства для этого подключения.

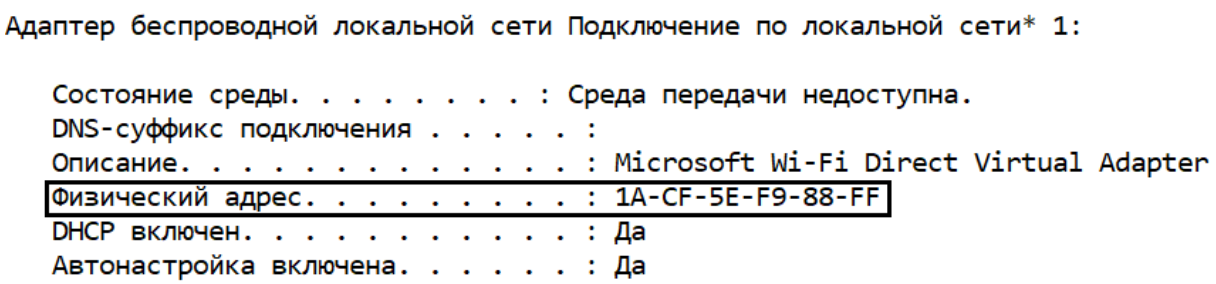


Рис. 3. Адаптер беспроводной локальной сети: подключение

Замечание: MAC-адрес устройства состоит из двенадцати шестнадцатеричных цифр и занимает 6 байтов (каждый байт – это блок из двух цифр, разделенных дефисами). Следовательно, всего может существовать $16^{12} = 2^{48} \approx 10^{14}$ различных физических адресов. Их распределением занимается организация IEEE Registration Authority. Производители получают диапазоны из $2^{24} \approx 16$ млн MAC-адресов (3 байта). В таком диапазоне фиксированы старшие три байта и могут принимать любое значение младшие три байта. Поэтому по трем старшим байтам MAC-адреса устройства можно определить его производителя (но стоит учитывать, что сейчас существуют способы изменить MAC-адрес).

За межсетевой уровень отвечает протокол IP (Internet Protocol, дословно «межсетевой протокол»). Этот протокол отвечает за определение IP-адресов, которые будут уникальными для каждого устройства, и позволяет компьютерам находить друг друга в сети. С помощью этого протокола компьютеры могут определить несколько возможных путей к конечному устройству. Наиболее популярными версиями протокола на сегодняшний день являются IPv4 и IPv6. Их различие заключается в том, что разработанный в 1981 г. IPv4 состоит из четырех байтов (32 бита), при записи значения байтов в десятеричной системе счисления разделяются точками. Всего таких IP-адресов может быть $(2^8)^4 = 2^{32} \approx 4.2$ млн. Со временем этот лимит начал исчерпываться, и к 2011 г. стал актуален переход на IPv6, который был разработан в 1999 г. Он занимает 16 байтов (128 битов) и записывается блоками по 2 байта в шестнадцатеричной системе счисления, разделенными двоеточием. Таких адресов может быть $(2^8)^{16} = 2^{128} \approx 3{,}4 \cdot 10^{38}$. IPv6 со временем будет использоваться больше, чем IPv4, но пока переход на новый протокол ограничен необходимостью реорганизации сети и модификации оборудования, что является дорогостоящей процедурой.

В отличие от MAC-адресов, которые выдаются каждому устройству индивидуально, IP-адреса бывают статические и динамические. Статические IP-адреса выдаются провайдером на постоянной основе (за дополнительную плату) либо задаются в настройках устройства (если устройство выполняет роль сервера). Динамические

выдаются временно только на период выхода в сеть. После выхода из сети IP-адрес освобождается и может быть выдан другому устройству. У каждого интернет-провайдера есть свой список свободных IP-адресов. При повторном подключении может сохраняться прежний IP-адрес, если он не был занят. Так что для простых пользователей «вычисление по IP» – не более чем сказка. На таких сайтах, как http://wwhois.ru/ip.php, можно узнать место, в котором официально зарегистрирован IP-адрес, но никто, кроме провайдера (организации, предоставляющей доступ к сети Интернет), не знает, кем этот IP-адрес используется. Провайдер может предоставить эту информацию только по решению суда, если имел место неправомерный доступ к данным или распространение запрещенных законом материалов. Вычислить получится не более чем регион нахождения, ведь списки IP-адресов провайдеры делят по регионам.

Исключение составляют ситуации использования средств анонимности в интернете, которые будут затронуты позже. Для того чтобы узнать свой IP-адрес, в ОС Windows введите в командную строку ipconfig. Вы увидите IPv4 и IPv6 для текущего подключения к сети.

```
DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::b52d:e519:6001:8915%13
IPv4-адрес. . . . . . . . . . . . : 192.168.100.6
Маска подсети . . . . . . . . . . : 255.255.255.0
Основной шлюз. . . . . . . . . . . : fe80::1%13
```

Рис. 4. Адаптер беспроводной локальной сети

На межсетевом уровне используется также протокол ICMP (Internet control message protocol, в пер. «протокол межсетевых управляющих сообщений»). Он нужен для обмена сообщениями между устройствами. Например, это могут быть сообщения о том, что маршрутизатор не работает или услуга недоступна. Это вспомогательный протокол, который используется в том числе для уменьшения количества потерянных при пересылке пакетов данных. Ниже приведены основные типы ICMP-сообщений (табл.2).

Таблица 2

Основные типы ICMP-сообщений

Тип сообщения	Описание
Адресат недоступен	Пакет не может быть доставлен
Время истекло	Время жизни пакета упало до нуля
Проблема с параметром	Неверное поле заголовка
Гашение источника	Сдерживающий пакет
Переадресовать	Научить маршрутизатор географии
Запрос отклика	Спросить машину, жива ли она
Отклик	Да, я жива
Запрос временного штампа	То же, что и Запрос отклика, но с временным штампом
Отклик с временным штампом	То же, что и Отклик, но с временным штампом

Посмотреть работу протокола можно в командной строке Windows, введя команду ping или tracert, а далее имя интересующего сайта или IP-адрес. Утилита ping проверяет доступность указанного узла, отправляя несколько пакетов и проверяя, были ли они доставлены.

```
C:\>ping yandex.ru

Обмен пакетами с yandex.ru [5.255.255.80] с 32 байтами данных:
Ответ от 5.255.255.80: число байт=32 время=41мс TTL=53
Ответ от 5.255.255.80: число байт=32 время=43мс TTL=53
Ответ от 5.255.255.80: число байт=32 время=47мс TTL=53
Ответ от 5.255.255.80: число байт=32 время=41мс TTL=53

Статистика Ping для 5.255.255.80:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 41мсек, Максимальное = 47 мсек, Среднее = 43 мсек
```

Рис. 5. Утилита Ping

Команда tracert (сокр. от англ. traceroute – «трассировка», от англ. trace route – «след маршрута») предназначена для определения маршрута следования данных в сети TCP/IP. Некоторые узлы могут не отвечать на такой запрос из-за того, что они для этого не предназначены. Поскольку маршрут к конечному узлу может измениться во время трассировки, полученный список узлов не обязательно принадлежит одному маршруту.

```
C:\>tracert yandex.ru

Трассировка маршрута к yandex.ru [5.255.255.80]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  192.168.100.1
  2    10 ms     7 ms    22 ms  87.226.151.27
  3     4 ms     3 ms     3 ms  79.133.87.194
  4    55 ms     7 ms     4 ms  79.133.87.145
  5    44 ms    48 ms    39 ms  87.226.183.89
  6    44 ms    40 ms    39 ms  5.143.250.94
  7    42 ms    41 ms    41 ms  yandex.ru [5.255.255.80]

Трассировка завершена.
```

Рис. 6. Трассировка маршрута

На транспортном уровне мы познакомимся с протоколами TCP и UDP. Задача TCP (Transmission control protocol, в пер. с англ. «протокол управления передачей») – управление передачей данных.

Сети ненадежны – из-за большого количества путей пакеты могут приходить не в том порядке или даже теряться. Протокол TCP обеспечивает правильный порядок получения пакетов и досылает потерянные пакеты данных. Это достигается следующим образом: каждому пакету данных присваивается порядковый номер, вместе с пакетом пересылается его контрольная сумма (значение, с большой вероятностью различное для двух разных пакетов). Получатель вычисляет свою контрольную сумму пакета и сравнивает ее с присланной. Если контрольные суммы совпали, то получатель отправляет подтверждение получения пакета с данным номером. В случае если пакет не дойдет (или дойдет

поврежденным), отправитель не получит подтверждения и отправит пакет снова. TCP использует множество приложений, например, SSH, WWW, FTP и мн. др.

UDP (User datagram protocol, в пер. с англ. «пользовательский протокол данных») похож на TCP, но он не проверяет полученные данные на правильность. И это не всегда плохо, ведь такая передача данных происходит быстрее. UDP полезно применять при воспроизведении видео, в аудио- и видеозвонках, сетевых играх, т.е. в тех задачах, информация в которых должна быть получена не позднее определенного времени.

Следующие протоколы относятся к прикладному уровню. HTTP (Hypertext transfer protocol, в пер. с англ. «протокол передачи гипертекста») обеспечивает загрузку сайтов в интернете. Клиент (устройство, на котором вы хотите загрузить сайт) отправляет запрос на веб-сервер (компьютер большой мощности, обеспечивающий работу большого количества клиентов с сайтом). Веб-сервер формирует ответ на запрос и отправляет его клиенту. HTTP отвечает за обмен данными между клиентом и сервером.

Протокол HTTP был разработан в 1992 г. и никак не защищал данные от возможного перехвата. Поэтому было разработано расширение HTTPS (Hypertext transfer protocol secure, в пер. с англ. «защищенный протокол передачи гипертекста»), позволяющее шифровать передаваемые данные. В настоящее время в основном используется защищенная версия протокола.

FTP (File transfer protocol, в пер. с англ. «протокол передачи файлов») – это протокол передачи файлов, появившийся задолго до HTTP, в 1971 г. Он работает на уровне приложений и обеспечивает одновременную передачу нескольких файлов между устройствами. FTP – небезопасный, поэтому не рекомендуется его применять для личных данных.

Протокол DNS (Domain name system, в пер. с англ. «система доменных имен») позволяет обращаться к интернет-ресурсам, указывая их адрес, например, yandex.ru вместо IP-адреса.

Для того чтобы упорядочить полученные знания, приводим в табл.3 соответствия рассмотренных протоколов уровням модели TCP/IP.

Таблица 3

Соответствия протоколов

Уровень модели TCP/IP	Протоколы
Прикладной	FTP, DNS, HTTP
Транспортный	TCP, UDP
Межсетевой	IP, ICMP
От хоста к сети	MAC

Источники:

Танненбаум Э. Компьютерные сети. 4-е изд. М.; СПб.: Питер, 2003.

Основы сетей и протоколов Интернет // Losst. [2017–2017]. Дата обновления: 9.02.2017. URL:

https://losst.ru/osnovy-setej-i-protokolov-internet (дата обращения: 16.08.2018).

7 уровней модели OSI – физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной // Infoprotect. [2016–2016]. Дата обновления: 05.03.2016. URL: http://infoprotect.net/protect_network/7-urovnej-modeli-osi-fizicheskij-kanalnyj-setevoj-transportnyj (дата обращения: 16.08.2018).

Анонимность в Интернете

Анонимность в Интернете подразумевает совершение различных действий в сети Интернет пользователем без раскрытия личности этого пользователя. Анонимность может служить для разных целей. Преступники могут распространять компьютерные вирусы, заниматься рассылкой спама или сообщений с угрозами, оставаясь при этом неузнанными. Законопослушным людям анонимность позволяет защищать персональные данные, в том числе обсуждать такие вещи, говоря о которых не хочется раскрывать свое имя (например, обсуждать свою личную жизнь).

Не имея под рукой программных и технических средств, самостоятельно мы можем добиться поверхностной, частичной анонимности. Например, при общении с другими людьми в социальной сети мы можем скрыть свои настоящие имя и фамилию, не выкладывать собственные фотографии и не сообщать собеседникам информацию, которая может каким-либо образом помочь

нас идентифицировать. Использование программных и технических средств, речь о которых пойдет далее, поможет нам получить более высокий уровень анонимности, т.к. они позволяют частично скрыть местоположение в сети. Полная же анонимность в сети Интернет, вероятно, невозможна, т.к. теоретически, используя IP-адрес, можно отследить местоположение любого устройства, подключенного к сети Интернет, и вычислить реального человека.

Прокси-сервера

Прокси-сервер – это промежуточный сервер между устройством пользователя и сервером интернет-ресурса. При обычном пользовании интернет-ресурсами мы подключаемся к их серверам напрямую, сервер «видит» наш IP-адрес. Помимо того что по IP-адресу владельцы ресурса могут определить наше местоположение, они также могут ограничить пользование ресурсом (наш интернет-провайдер может, например, заблокировать доступ к серверам некоторых интернет-ресурсов).

При использовании прокси-сервера мы посылаем запрос с нашего устройства прокси-серверу, который (уже от себя, с использованием своего IP-адреса) посылает запрос серверу интернет-ресурса. Когда прокси-сервер получает ответ на свой запрос, он пересылает его на наше устройство. Таким образом, использование прокси-сервера позволяет скрыть наш IP-адрес от владельцев

интернет-ресурсов. Однако при наличии специального оборудования наш IP-адрес все еще можно отследить.

Схема работы прокси-сервера приведена на рис. 7.

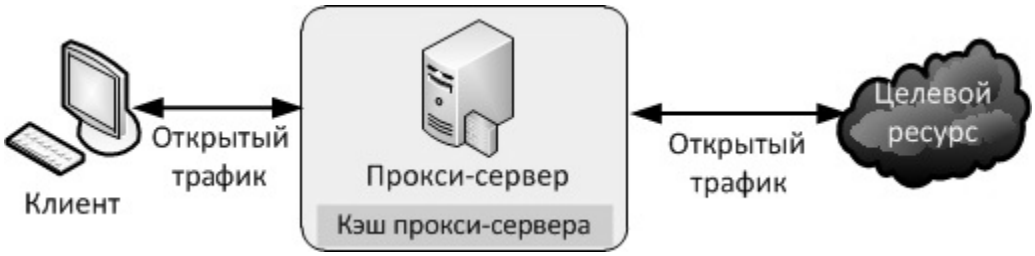


Рис. 7. Схема работы прокси-сервера

VPN

VPN (Virtual Private Network, в пер. с англ. «виртуальная частная сеть») – это частная сеть, в которую входят только определенные устройства и которая располагается поверх сети Интернет. Примером VPN может являться ваша домашняя сеть. Наверняка у вас дома имеется Wi-Fi-роутер, к которому подключены ваши устройства. Все эти устройства могут общаться между собой с помощью роутера, даже если сам роутер не подключен к сети Интернет. В различных компаниях VPN используется для того, чтобы обеспечить безопасное подключение между отделениями соответствующей компании, которые находятся на большом расстоянии друг от друга, или для того, чтобы обеспечить безопасное подключение для сотрудников, работающих удаленно. Организуется такая сеть следующим образом: в офисе компании располагается VPN-сервер. Все, кто желает подключиться к данной VPN-сети, должны знать адрес VPN-сервера, а также логин и пароль для подключения.

Кроме того что владелец VPN-сервера контролирует, какие именно устройства могут подключиться к сети, он также контролирует весь трафик подключенных к сети устройств. Как правило, соединение между устройством, входящим в сеть VPN, и VPN-сервером является шифрованным.

Схема работы VPN приведена на рис. 8.

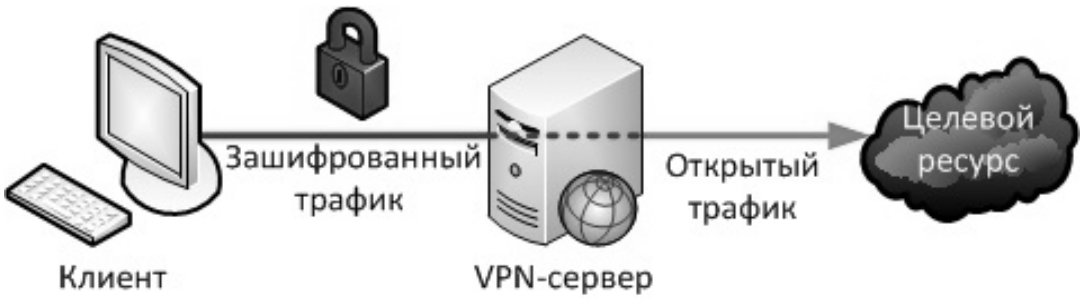


Рис. 8. Схема работы VPN

TOR

TOR (The Onion Router) – это свободно распространяемое ПО для реализации луковой маршрутизации. Луковая маршрутизация – это технология, позволяющая анонимно обмениваться данными в сети. Построена она следующим образом: каждый пользователь TOR устанавливает на своем устройстве прокси-сервер, который подключен к серверам TOR и связан с прокси-серверами других пользователей TOR. Таким образом, система состоит из множества связанных прокси-серверов. Когда один из пользователей хочет получить доступ к какому-либо интернет-ресурсу, система случайным образом выбирает три узла (иначе они называются еще нодами от англ. node – «звено»), через которые пакет с запросом

пользователя пройдет по пути к целевому ресурсу. Кроме того, пакет с запросом пользователя последовательно шифруется тремя ключами (по одному на каждый из узлов, через который он будет проходить). Шифрование происходит в три итерации по аналогии с тремя слоями луковицы таким образом, чтобы каждый из узлов знал только то, куда отправить пакет дальше. После того как пакет попадает на первый из узлов, узел расшифровывает верхний слой и узнает, какому узлу необходимо передать пакет. Второй и третий сервера выполняют аналогичные действия.

Схема работы TOR приведена на рис. 9.

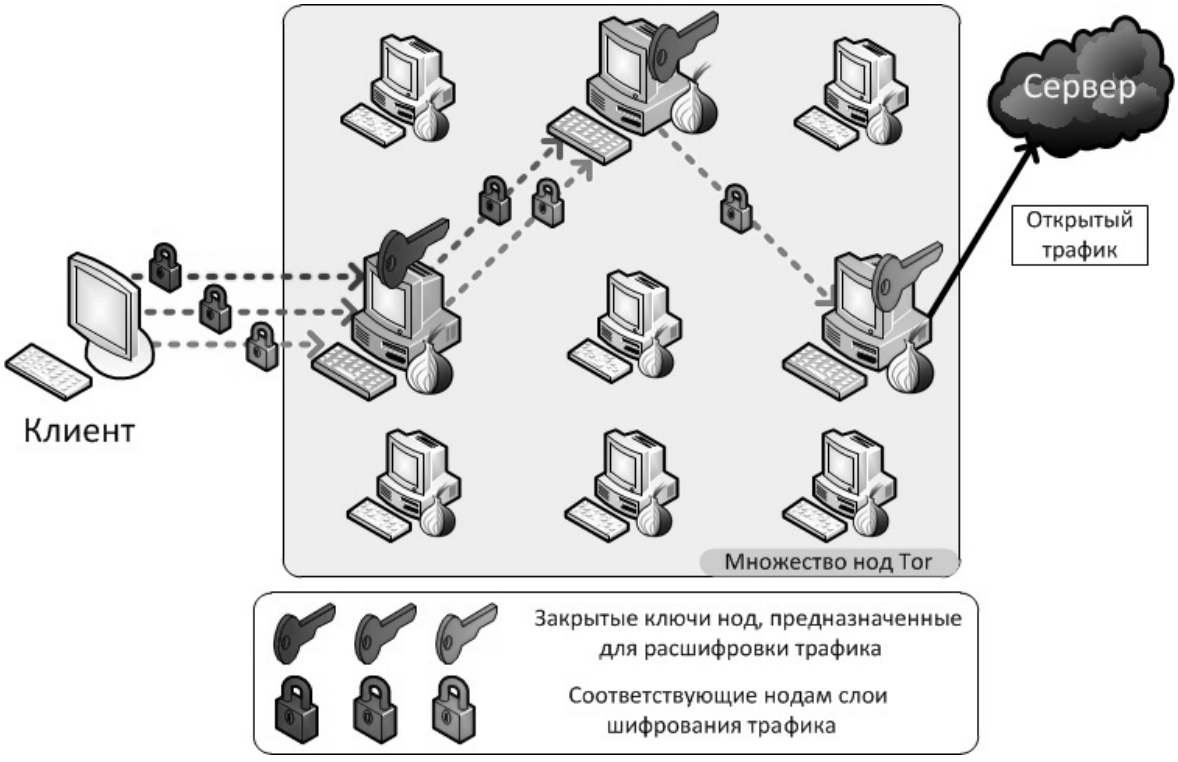


Рис. 9. Схема работы TOR

Источники:

Волоцкий М. Что такое прокси-серверы и как ими пользоваться // Лайфхакер. [2018–2018]. Дата обновления: 26.04.2018. URL: https://lifehacker.ru/proksi-servery/ (дата обращения: 14.08.2018).

Суягин С. Что такое VPN // Лайфхакер. [2018–2018]. Дата обновления: 17.04.2018. URL: https://lifehacker.ru/chto-takoe-vpn/ (дата обращения: 14.08.2018).

Tor // Википедия. [2018–2007]. Дата обновления: 08.09.2018. URL: https://ru.wikipedia.org/?oldid=94951806 (дата обращения: 14.08.2018).

Методы анонимности в сети. Ч. 1: Просто о сложном // habr. [2013–2013]. Дата обновления: 17.08.2013. URL: https://habr.com/post/190396/ (дата обращения: 14.08.2018).

Виды сетевых атак

Сетевая атака – это действия киберпреступников, направленные на получение контроля над атакуемой системой, выведение системы из строя (отказ в обслуживании) или получение данных пользователей этой системы. Рассмотрим основные виды сетевых атак и способы защиты от них.

Mailbombing

Суть атаки проста: на почтовый ящик жертвы посылается огромное количество писем. Это вызывает отказ работы данного почтового ящика или даже всего почтового сервиса.

Способы защиты

1. Давать адрес электронной почты только проверенным людям.
2. Указывать адрес электронной почты только на проверенных интернет-ресурсах.

Переполнение буфера

Данная атака основывается на поиске злоумышленником уязвимостей атакуемой системы, которые позволят вызвать нарушение границ памяти и аварийно завершить приложение или выполнить код, введенный пользователем.

Способы защиты

3. Исправление кода программы для устранения уязвимостей.
4. Использование запрета исполнения кода, который находится в буфере.
5. Использование в коде программы проверок выхода за границы памяти.

Использование вирусных программ

Такой тип атаки построен на использовании рассмотренных нами ранее вирусных программ (файловых вирусов, троянских программ, шпионских программ, руткитов и пр.) для выведения системы из строя или получения необходимой информации.

Способы защиты

1. Использование антивирусных программ и своевременное обновление их баз.
2. Использование межсетевых экранов.

IP-спуфинг

IP-спуфинг заключается в том, что злоумышленник выдает себя за пользователя, обладающего некоторыми правами доступа/управления в атакуемой системе. Для этого злоумышленник может воспользоваться любым авторизованным IP-адресом, т.е. тем адресом, которому разрешен доступ к определенным сетевым ресурсам системы. Обычно такой вид атак ограничивается вставкой злоумышленником ложной информации или вредоносных команд в поток данных между сервером и клиентом.

Способ защиты – правильная настройка управления доступом к системе (например, отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри сети).

Man-in-the-middle (человек посередине)

Для организации данного типа атаки злоумышленник должен получить доступ ко всем пакетам, передаваемым атакуемой системой по сети. Сама же атака заключается в краже информации, искажении передаваемых данных и их анализе для получения сведений о системе и ее пользователях.

Способ защиты – шифрование данных.

Инъекции

Инъекции – это атаки, в ходе которых злоумышленник пытается получить контроль над системой путем внедрения в код серверного приложения собственного вредоносного кода или пытается получить/удалить некоторые данные из базы данных путем изменения параметров запроса к ней.

Способы защиты

1. Использование в коде программы проверок получаемых от пользователя данных.
2. Исправление кода программы для устранения уязвимостей.

Отказ в обслуживании (Dos и DDos-атаки)

Dos и DDos-атаки – это атаки на компьютерные системы путем одновременного отправления большого количества запросов с множества компьютеров с целью перегрузки атакуемой системы, вывода ее из строя.

Способ защиты – правильная настройка и использование антиDos-функций сетевых экранов и маршрутизаторов.

Phishing-атаки

Фишинг – это обман пользователей с целью получения информации о них (или об организации, в которой они работают), логинов, паролей, данных банковских карт и пр. Чаще всего для введения пользователя в заблуждение злоумышленники используют

электронную почту. Например, пользователю приходит письмо якобы из банка о том, что банк обновил систему безопасности и всем владельцам карт нужно подтвердить информацию о себе и о своей банковской карте, введя данные на сайте банка. В письме обычно содержится ссылка на сайт злоумышленников, который может быть очень похож на официальный и по оформлению, и по адресу (например, отличаться одной буквой). Как только пользователь введет данные, они тут же окажутся в руках злоумышленников.

Способ защиты – использовать только проверенные сайты интернет-ресурсов и заходить на них напрямую.

Источники:

Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). Уфа: Лето, 2011. С. 8–13. URL: https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 16.08.2018).

Глава 4

Личная гигиена при работе за компьютером

Правильная организация рабочего места за компьютером

От правильной организации рабочего места зависит не только удобство работы за компьютером, но и здоровье в целом. В частности, на наше здоровье могут оказывать влияние такие факторы, как освещенность рабочего места, правильная поза сидящего, правильное расположение монитора и т.п.

Далее будут представлены некоторые рекомендации с целью правильной организации рабочего места за компьютером.

Освещенность рабочего места

Необходимо отрегулировать освещенность рабочего места таким образом, чтобы глазам было комфортно. Свет не должен быть слишком ярким, но также нежелательна и темнота.

Перед началом работы за компьютером нужно убедиться в отсутствии отражений (бликов) на экране монитора.

Следует также убедиться в отсутствии встречного светового потока. Свет из окна не должен попадать прямо в глаза пользователю. Для решения такой проблемы можно использовать шторы или жалюзи на окнах.

Монитор

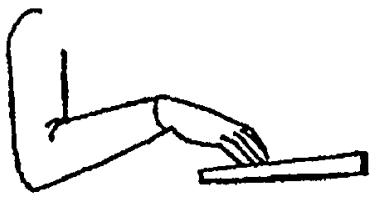
Важной частью организации рабочего места является правильное расположение монитора компьютера.

Монитор нужно располагать прямо перед пользователем, оптимальное расстояние от монитора до глаз пользователя должно быть 60–70 см (но не ближе 50 см).

Чтобы ослабить напряжение мышц шеи и спины, центр экрана монитора должен располагаться прямо напротив глаз или же чуть ниже.

Клавиатура

Клавиатура должна размещаться таким образом, чтобы было удобно пользователю, т.е. прямо перед пользователем. Лежать она должна устойчиво, отступив от края поверхности 10–30 см.



Положения запястья и кисти руки при работе на клавиатуре:
а - правильное при наличии опорной планки для кисти руки;
б - неправильное

Рис. 10. Примеры положения рук

Рабочий стол и кресло

Большое значение имеют также рабочий стол и кресло, за которыми сидит пользователь. В связи с этим к рабочему столу и креслу есть некоторые рекомендации, которые также нужно выполнять.

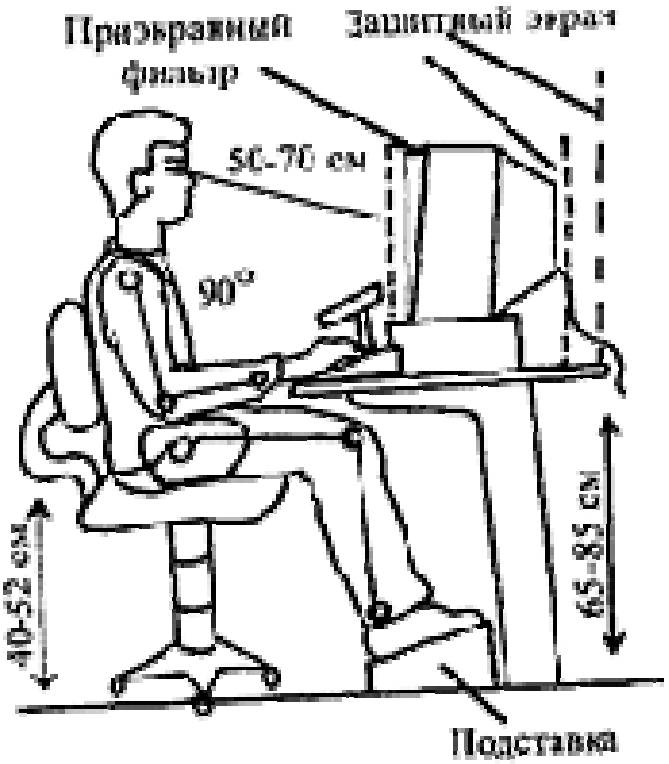


Рис. 11. Правильная посадка

Высота стола должна быть в пределах 68–85 см, оптимальная высота стола – 72,5 см.

Желательные размеры поверхности рабочего стола для компьютера: длина – 80–120 см, ширина – 80–100 см.

Рабочий стол должен иметь пространство для ног высотой не менее 70 см, шириной не менее 50 см, глубиной на уровне колен не менее 45 см и на уровне вытянутых ног не менее 65 см.

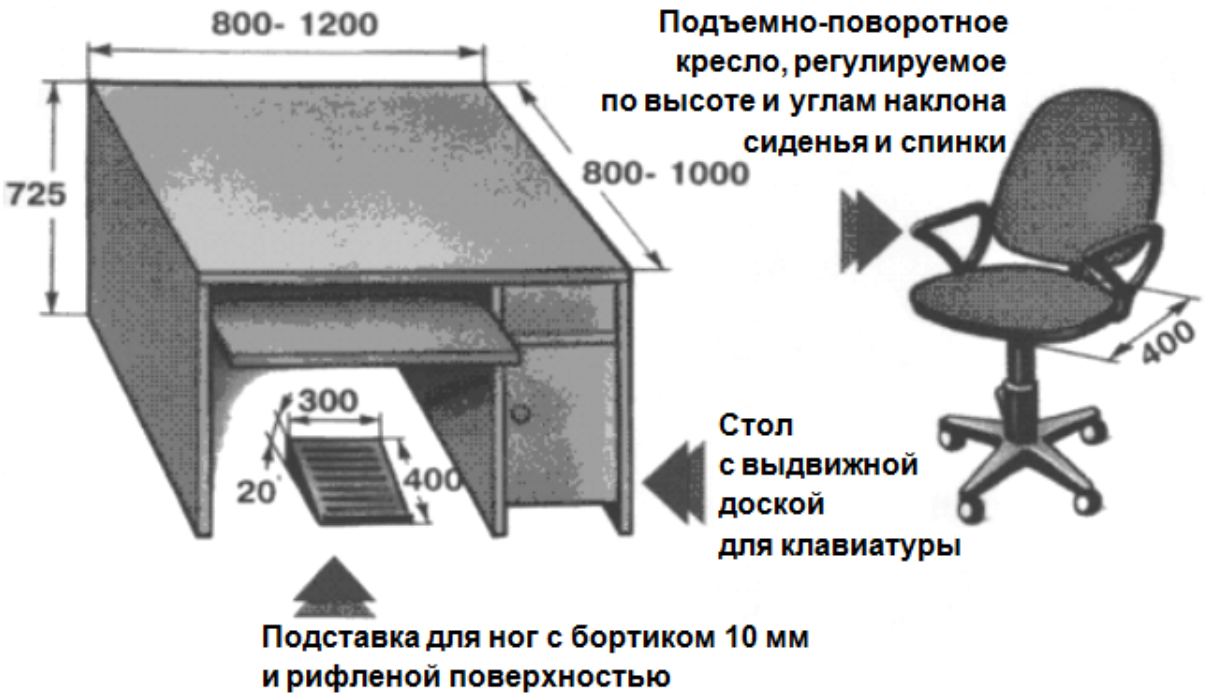


Рис. 12. Требования к конструкции кресла и стола

Конструкция рабочего кресла должна обеспечивать рациональную рабочую позу пользователя, давать возможность изменять ее с целью снижения статического напряжения мышц шейно-плечевой области и спины.

Тип рабочего кресла должен выбираться в зависимости от характера и продолжительности работы. Обязательно при выборе кресла необходимо учитывать рост пользователя.

Кресло должно быть подъемно-поворотным, регулируемым по высоте и желательно по углам наклона сиденья и спинки, а также по расстоянию от спинки до переднего края сиденья.

- Ширина и глубина сиденья должна быть не менее 40 см, с закругленным передним краем.
- Высота опорной поверхности спинки должна быть 30 ± 2 см, ширина не менее 38 см.

- Угол наклона спинки в вертикальной плоскости должен быть в пределах 0 ± 30°.
- Желательно, чтобы кресло имело регулируемые стационарные или съемные подлокотники.

Рабочее место пользователя целесообразно оборудовать подставкой для ног шириной не менее 30 см, глубиной не менее 40 см и углом наклона опорной поверхности подставки до 20°. Для большего удобства поверхность подставки может быть рифленой и иметь по переднему краю бортик высотой 1 см.

Положение тела

Длительное нахождение человека в фиксированной позе при сидячей работе за компьютером нагружает определенные группы мышц, другие же мышцы, наоборот, ослаблены, поэтому необходимо соблюдать правильное положение тела человека за рабочим местом, что поможет снять напряжение с позвоночника.

Наиболее удобным для пользователя является вертикальное, слегка отклоненное назад положение.

Положение тела пользователя должно соответствовать направлению взгляда.

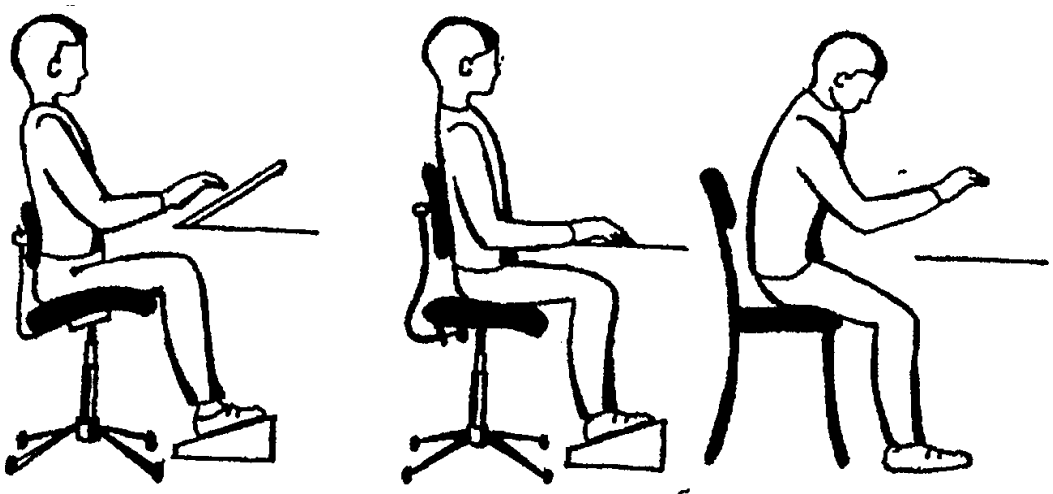


Рис. 13. Примеры положения тела пользователя

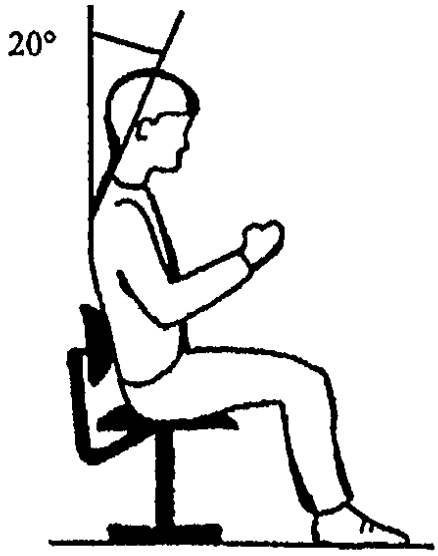


Рис. 14. Оптимальный наклон головы

Во время работы за компьютером нужно следить за правильной рабочей позой. На протяжении всего рабочего времени необходимо:

- не сутулиться;
- не сидеть, положив ногу на ногу;

- стараться сохранять прямые углы в локтевых, тазобедренных, коленных и голеностопных суставах;
- найти такое положение головы, при котором шея устает меньше всего, и в соответствии с этим положением отрегулировать кресло, расположение монитора, высоту подставки для ног.

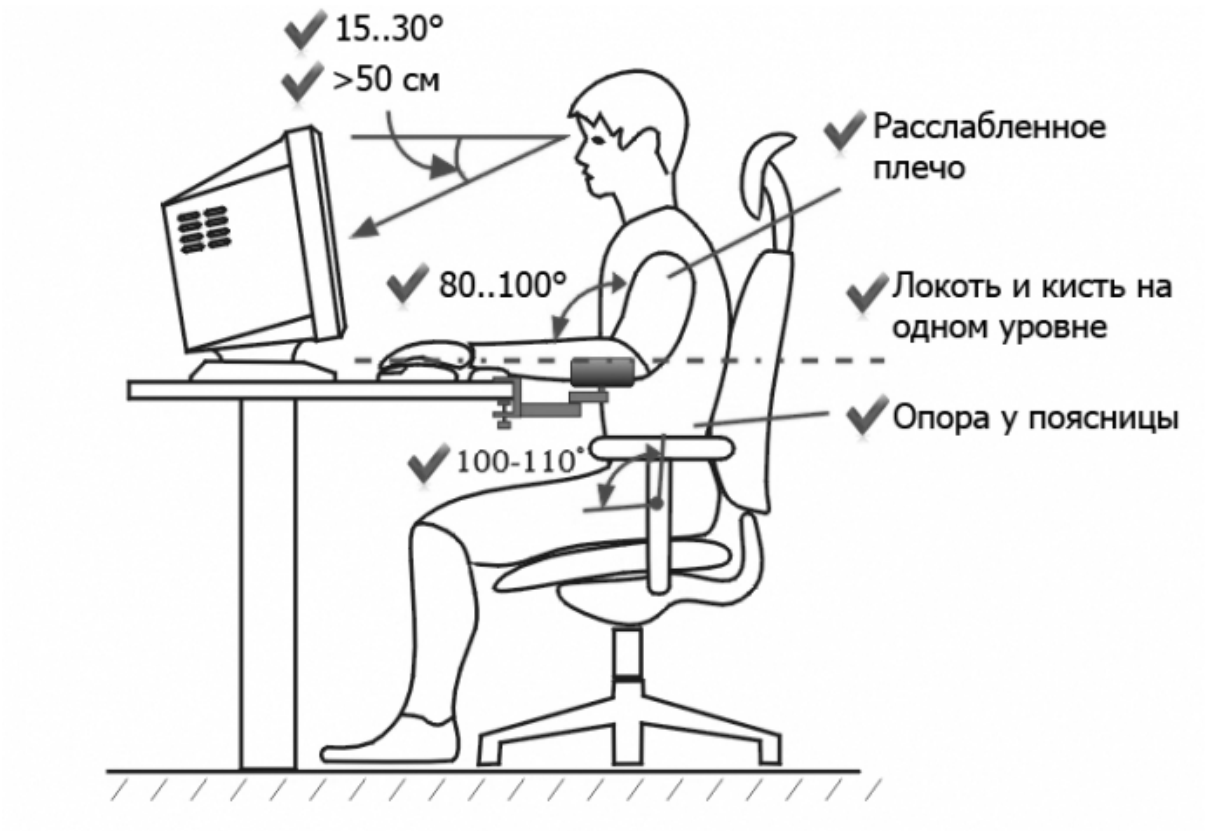


Рис. 15. Требования к положению тела пользователя для комфортной работы за комьютером

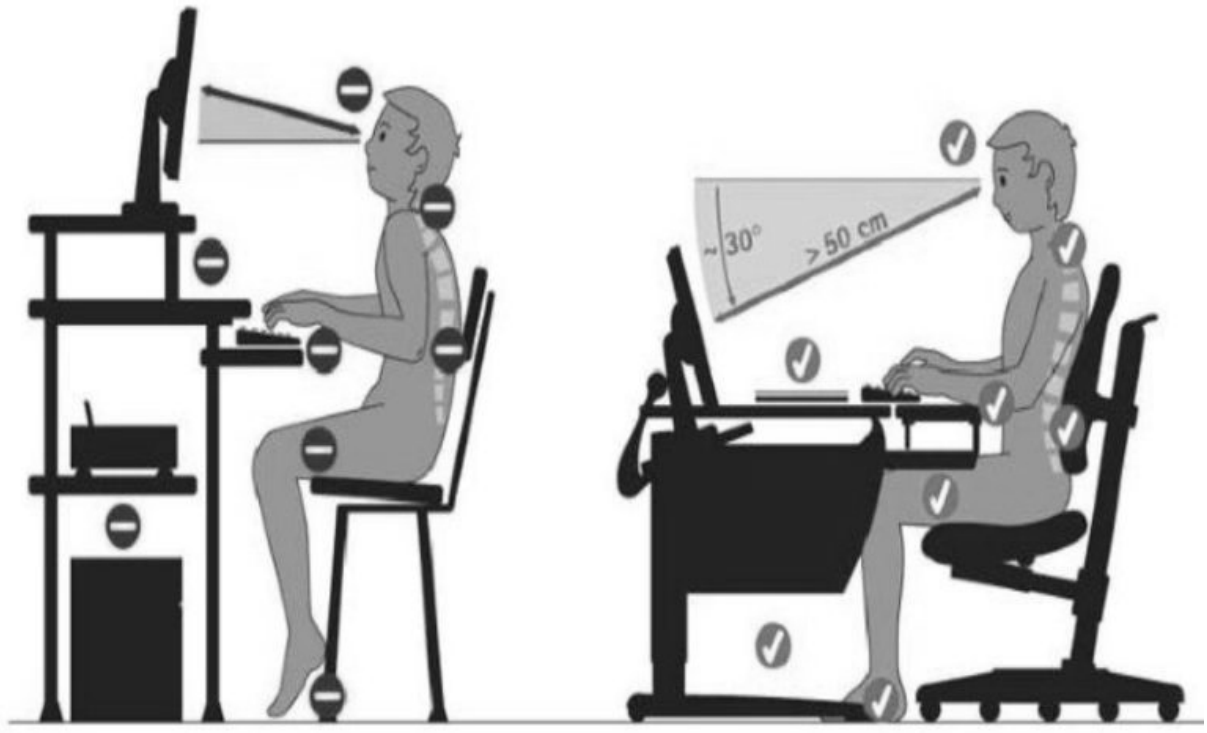


Рис. 16. Расположение тела при работе за компьютером

Оптимальный режим работы за компьютером

Поскольку долгая работа за компьютером отрицательно влияет на зрение человека, рекомендуется через каждый час интенсивной работы устраивать перерыв длительностью 15 мин., если же работа менее интенсивная, то перерыв можно делать через каждые 1,5-2 часа. Эффективность таких перерывов повышается, если сочетать их с гимнастикой для глаз.

Таким образом, при работе за компьютером следует принять во внимание полезные советы:

1. Важно правильно организовать свое рабочее место за компьютером.
2. Необходимо соблюдать паузы при работе за компьютером.
3. Желательно делать гимнастику для глаз.

Источники:

Фирсова К. 10 советов для здоровой работы за компьютером // КТО?ЧТО?ГДЕ? [2018–2018]. Дата обновления: 28.02.2018. URL: http://kto-chto-gde.ru/story/10-sovetov-dlya-zdorovoj-raboty-za-kompyuterom/ (дата обращения: 21.08.2018).

Организация рабочего места за компьютером // СПЕЦ КОМП. [2014–2014]. Дата обновления: 28.11.2014. URL: https://spec-komp.com/news/organizacija_rabochego_mesta_za_kompjuterom/2014-11-28-890 (дата обращения: 21.08.2018).

Типовая инструкция по охране труда для пользователей персональными электронно-вычислительными машинами (ПЭВМ) в электроэнергетике: РД 153-34.0-03.298-2001. Введ. с 01.05.2001. М.: ЭНАС, 2001.

Компьютерная зависимость

Когда человек начинает слишком много времени проводить за компьютером, может наступить компьютерная зависимость.

Термин «компьютерная зависимость» означает патологическое пристрастие человека к работе или проведению времени за компьютером. Впервые о компьютерной зависимости заговорили американские ученые в начале 80-х гг. Однако в наше время не все ученые признали этот термин, хотя данное явление приобретает все больший размах.

Причины возникновения компьютерной зависимости

Причин возникновения компьютерной зависимости достаточно много. К основным причинам можно отнести:

- Личностные качества: ранимость, тревожность, низкая самооценка, плохая стрессоустойчивость, замкнутость. Виртуальный мир дает человеку возможность стать идеальным, уйти от жизненных трудностей.
- Неудовлетворенность действительностью.
- Приучение родителями с детства использовать компьютер.
- Одиночество, отсутствие друзей в реальном мире.
- Особенности воспитания и взаимоотношений в семье.

Симптомы компьютерной зависимости

Симптомы (признаки) компьютерной зависимости можно разделить на две группы: психические и физические. Рассмотрим ниже, что входит в каждую из них.

К психическим признакам компьютерной зависимости относятся:

1. Потеря контроля над временем при работе за компьютером. Человек начинает проводить много времени за компьютером, при этом не осознавая этого.
2. Сильная зависимость настроения от нахождения за компьютером. Когда человек проводит время за компьютером, он испытывает чувство радости, у него хорошее настроение. Когда же у человека нет дос-

тупа к компьютеру, он становится агрессивным, не знает, чем себя занять.

3. Потеря интереса к социальной стороне жизни, к удовлетворению других потребностей: в пище, сне и др.
4. Высокая раздражительность в случаях, когда ограничивают время нахождения за компьютером, когда невозможно выйти в интернет, из-за поломки компьютера.

В группу физических признаков компьютерной зависимости входят:

1. Проблемы со зрением: синдром «сухого глаза», дисплейный синдром, ухудшение зрения. Чаще всего такие проблемы возникают вследствие длительного нахождения у монитора компьютера.
2. Нарушения опорно-двигательного аппарата: искривление позвоночника, проблемы с осанкой. Неправильная поза при сидении за компьютером с согнутой спиной иногда может привести даже к развитию остеохондроза или появлению межпозвоночных грыж. От постоянного напряжения мышц руки и пальцев при работе с мышкой может возникнуть мышечная боль, а иногда и карпальный синдром (ущемление нервов, сухожилий).
3. Проблемы с пищеварительной системой: нарушение питания, гастрит, язвенная болезнь, хронические запоры, геморрой. Такие проблемы возникают из-за нерегулярного и неполноценного питания, а также из-за постоянного нахождения в сидячем положении в ссутуленной позе.

4. Заболевания сердечно-сосудистой системы. Из-за малоподвижного образа жизни и длительного нахождения в сидячей позе может возникнуть застой крови, который приводит к развитию варикоза. А если вместе с этим еще и неправильно питаться, делать постоянные перекусы, то могут появиться холестериновые бляшки в сосудах, развиться атеросклероз.
5. Проблемы с нервной системой. Нервная система истощается вследствие того, что необходимо анализировать большие объемы информации, наступает утомление. Из-за отсутствия свежего воздуха, недосыпания, неправильного питания мозг не успевает отдыхать, а нервная система восстанавливаться. Поэтому утомление постепенно растет и переходит в хроническую усталость.

Физические признаки компьютерной зависимости чаще всего возникают из-за длительного пребывания человека за компьютером. Некоторые из них могут возникнуть и у человека, не страдающего компьютерной зависимостью, но вследствие некоторых причин вынужденного проводить много времени за компьютером.

Способы борьбы с компьютерной зависимостью

Для борьбы с компьютерной зависимостью важно, чтобы человек, ею страдающий, признал это и сам захотел от нее избавиться. В связи с этим в лечении данной зависимости основную роль играют психологи и психо-

терапевты. При этом важны также помощь и содействие родственников страдающего этой болезнью.

Для успешного лечения необходимо найти причину длительного времяпрепровождения за компьютером. Далее целью становится вовлечение человека, страдающего компьютерной зависимостью, в реальный мир, ограничить время использования компьютера.

Источники:

Компьютерная зависимость // tiensmed.ru. [2015–2015]. Дата обновления: 19.05.2015. URL: https://www.tiensmed.ru/programmer4.html (дата обращения: 19.08.2018).

Как избавиться от компьютерной зависимости // TutKnow.ru. URL: https://tutknow.ru/psihologia/7129-kak-izbavitsya-ot-kompyuternoy-zavisimosti.html (дата обращения: 19.08.2018).

Родительский контроль

Родительский контроль подразумевает комплекс правил и мер по предотвращению предполагаемого негативного воздействия компьютера и сети Интернет на ребенка.

Чтобы правильно организовать работу ребенка за компьютером, запретить использование определенных программ и сайтов, т.е. обеспечить родительский контроль, обычно используется специальное программное обеспечение, которое, в частности, может быть встроено.

При родительском контроле может использоваться ограничение по времени (например, использование компьютера в определенные часы в течение суток либо в

определенные дни), а также ограничение по определенным интернет-ресурсам нежелательной направленности (например, список сайтов, на которые ребенок не сможет зайти).

Родительский контроль можно разделить на активный и пассивный.

К пассивным видам родительского контроля относятся следующие методы:

- ограничение использования компьютера по времени (например, можно разрешить использовать компьютер в рабочие дни с 16:00 до 17:30, а в выходные с 12:00 до 18:00);
- ограничение на запуск программных продуктов (например, можно указать те программы, которыми может пользоваться ребенок; те программы, которых нет в этом списке, не могут быть запущены ребенком);
- ограничение на время использования той или иной программы (например, можно установить определенное время использования определенной программы);
- ограничение на посещение интернет-ресурсов:
  – посещение только определенных сайтов (т.е. только тех, которые указаны в списке);
  – запрет на посещение сайтов определенных тематик;
  – блокировка определенных сайтов для посещения.

К активным видам родительского контроля относится например, отслеживание контента сайтов, посещаемых ребенком.

Источники:

Родительский контроль // Википедия. [2010–2017]. Дата обновления: 02.10.2017. URL: https://ru.wikipedia.org/?oldid=88042501 (дата обращения: 13.08.2018).

Защита персональных данных в сети Интернет

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Так, если мы кому-то скажем свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь, будет затруднительно.

Получается, что персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, который позволяет вас идентифицировать.

В целом можно сказать, что персональные данные – это совокупность данных, которая необходима и достаточна для идентификации какого-то человека.

Чтобы защитить свои персональные данные в сети Интернет, нужно придерживаться следующих рекомендаций:

1. Ограничьте объем информации о себе, находящейся в Интернете. Не указывайте лишнюю личную информацию в социальных сетях, используйте настройки приватности.
2. Создайте 2 адреса электронной почты: частный (для переписки) и публичный (для открытой деятельности – форумов, актов и т.д.).
3. Не публикуйте онлайн-фотографии ваших документов, билетов и платежных чеков.
4. Не пользуйтесь открытыми точками доступа Wi-Fi и выключайте Wi-Fi на устройстве, если не собираетесь его использовать.
5. Включите двухфакторную аутентификацию на всех сайтах и сервисах, которые предусматривают эту возможность.
6. Не открывайте подозрительные вложения, присланные по электронной почте и через интернет-менеджеры.
7. Следите за тем, какие мобильные приложения используют личные данные.
8. Никогда не используйте одинаковые пароли на разных ресурсах.

9. Проверяйте интернет-адреса, по которым вы переходите с почты и с сайтов.
10. Установите на свой ПК защитное ПО и следите за регулярностью обновлений антивирусных баз.

Источники:

Персональные данные Дети. URL: http://персональные-данные.дети (дата обращения: 23.08.2018).

Правильное использование социальных сетей

В настоящее время социальные сети приобрели всеобщую популярность. Ими активно пользуются как взрослые, так и школьники. Но в то же время социальные сети таят в себе много опасностей. Поэтому важно следовать таким советам:

1. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
2. Контролируйте информацию, которую размещаете о себе в социальной сети.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.
4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства, номер школы или класса, посоветуйтесь с

родителями или взрослыми людьми, которым вы доверяете.

5. Используйте только сложные пароли, уникальные для каждой учетной записи или сервиса.
6. Меняйте пароли каждые полгода.
7. Используйте двухфакторную аутентификацию при входе в социальную сеть.
8. Если одного из ваших друзей взломали, вам может прийти сообщение с просьбой о помощи или о переводе денег на карту или номер телефона. Будьте осторожны, такое сообщение может быть написано злоумышленником. Постарайтесь связаться с другом и убедиться, что сообщение отправлено действительно им, прежде чем предпринимать какие-либо действия.

Одной из частых опасностей социальных сетей является взлом аккаунта. Взлом аккаунта может привести к краже персональных данных, ведению личной переписки от лица хозяина аккаунта, иногда к вымоганию денежных средств и шантажу. Поэтому очень важно защитить свой аккаунт. Если все-таки ваш аккаунт взломали, необходимо:

- получить доступ к аккаунту (при необходимости восстановить пароль);
- изменить пароль;
- в настройках безопасности завершить все текущие сеансы в данном аккаунте;

- исправить сделанные изменения в аккаунте (удалить написанные сообщения, удалить добавленных друзей и отменить заявки на добавление в друзья);
- проверить наличие других изменений (добавление или удаление фото, постов на стене, изменение личной информации) и при необходимости исправить их;
- если злоумышленником были проведены банковские операции, заблокировать карту и сообщить в банк о недействительности операции.

В случае отсутствия доступа к телефону, к которому привязан аккаунт (кража или потеря), обратиться в салон связи своего оператора для блокировки старой сим-карты и получения новой.

Заключение

Мы рассказали вам об основных угрозах для вашего компьютера, существующих на сегодняшний день, а также о средствах защиты от данных угроз. Разумеется, это далеко не полный список, т. к. киберпреступность непрерывно развивается, как и безопасность компьютерных систем. Но, используя приведенные в данной книге советы, вы сможете защититься от большинства возможных атак, защитить информацию, хранящуюся на вашем компьютере, безопаснее чувствовать себя на просторах интернета.

В заключение мы приведем пример создания системы защиты информации (СЗИ) для домашнего компьютера. Данный пример показывает, как создаются подобные системы специалистами по компьютерной безопасности, работающими в различных организациях.

Создание любой системы защиты информации (СЗИ) проходит следующие этапы:

1. Определение информации, которая подлежит защите.
2. Выявление угроз и каналов утечки информации.
3. Проведение оценки уязвимости от этих угроз и рисков.
4. Определение требований к СЗИ.
5. Осуществление выбора средств защиты.
6. Внедрение и использование выбранных мер и средств.
7. Контроль целостности и управление защитой.

На первом этапе определяется вся информация, подлежащая защите. Для персонального компьютера это:

1. Личные документы, файлы.
2. Аккаунты в соцсетях, интернет-магазинах, электронных кошельках и пр., а также пароли от них.
3. Файлы операционной системы.

На следующем этапе необходимо определить, каким угрозам может быть подвержена информация, а также через какие каналы утечки эти угрозы могут быть реализованы. Ниже приведена табл.4 с возможными угрозами и каналами утечки информации.

Таблица 4

Возможные угрозы и каналы утечки информации

Информация, подлежащая защите	**Угрозы информации**	**Каналы утечки информации**
1. Личные документы, файлы	Получение, использование и распространение личных документов и файлов сторонним лицом. 0,79 -> 0,47 Повреждение личных документов и файлов. 0,43 -> 0,31	Получение доступа к ПК сторонним лицом. Вирусные атаки. Ошибки пользователя. Программные ошибки. Программные ошибки.
2. Аккаунты в соц. сетях, интернет-магазинах, электронных кошельках	Получение, использование и распространение личной информации и получение доступа к	Получение доступа к ПК сторонним лицом. Вирусные атаки.

Окончание табл. 4

и пр., а также пароли от них	различным аккаунтом сторонним лицом. 0,85 -> 0,38	Ошибки пользователя.
3. Файлы операционной системы	Повреждение файлов операционной системы. 0,27 -> 0,17	Получение доступа к ПК сторонним лицом. Вирусные атаки. Ошибки пользователя. Программные ошибки.

После определения угроз и каналов утечки информации производится оценка уязвимости от этих угроз и устанавливается требование к СЗИ по необходимому уровню снижения данных угроз (то значение, которого мы должны достигнуть после применения созданной СЗИ). Оценки уязвимостей и значения требований к СЗИ приведены в той же табл. 4. Записываются они непосредственно под видом угрозы следующим образом: значение уязвимости -> значение требования к СЗИ. Значение уязвимости – вещественное число в пределах от 0 до 1, которое выражает нашу уверенность в том, что данная угроза будет реализована. Значение требования к СЗИ – также вещественное число в пределах от 0 до 1, которое является нашей уверенностью в том, что данная угроза будет реализована после применения созданной СЗИ.

Далее необходимо выбрать средства защиты, которые помогут уменьшить вероятность осуществления обнару-

женных угроз. Средства защиты записываются в таблицу в порядке убывания значения уязвимости.

Таблица 5

Краткий план создания системы защиты информации

Угроза	**Средства защиты**	**Дата выполнения, стоимость работ**
Получение, использование и распространение личной информации и получение доступа к различным аккаунтом сторонним лицом	Использовать для авторизации в ОС пароль, состоящий из не менее чем 8 символов, включающих не менее одной буквы верхнего и нижнего регистра латинского алфавита и не менее одной цифры. Установить антивирусную программу на компьютер.	13.08.2018 0 руб. 13.08.2018 1290 руб.
Получение, использование и распространение личных документов и файлов сторонним лицом	Использовать для авторизации в ОС пароль, состоящий из не менее чем 8 символов, включающих не менее одной буквы верхнего и нижнего регистра латинского алфавита и не менее одной цифры. Установить антивирусную программу на компьютер. Проверка и настройка ПО специалистом.	13.08.2018 0 руб. 13.08.2018 1290 руб. 14.08.2018 1000 руб.
Повреждение личных документов и файлов	Использовать для авторизации в ОС пароль,	13.08.2018 0 руб.

Окончание табл. 5

	состоящий из не менее чем 8 символов, включающих не менее одной буквы верхнего и нижнего регистра латинского алфавита и не менее одной цифры. Установить антивирусную программу на компьютер. Покупка внешнего носителя для резервного копирования и обновление на нем резервных копий необходимых документов и файлов 1 раз в неделю. Проверка и настройка ПО специалистом.	 13.08.2018 1290 руб. 15.08.2018 3500 руб. 14.08.2018 1000 руб.
Повреждение файлов операционной системы	Использовать для авторизации в ОС пароль, состоящий из не менее чем 8 символов, включающих не менее одной буквы верхнего и нижнего регистра латинского алфавита и не менее одной цифры. Установить антивирусную программу на компьютер. Настройка резервного копирования ОС для периодического создания точек восстановления. Проверка и настройка ПО специалистом.	13.08.2018 0 руб. 13.08.2018 1290 руб. 15.08.2018 0 руб. 14.08.2018 1000 руб.

Затем следует внедрение и использование выбранных мер и средств. В этом пункте необходимо подсчитать общую стоимость разработки СЗИ.

Общая стоимость созданной СЗИ: 5790 руб.

Последним пунктом является контроль целостности и управление защитой. Здесь нужно описать действия, которые следует выполнить в случае реализации угроз.

В случае взлома аккаунта необходимо:

1. Получить доступ к аккаунту (при необходимости восстановить пароль).
2. Изменить пароль.
3. Проверить, были ли внесены какие-либо изменения, и исправить их.

В случае получения злоумышленниками доступа к компьютеру необходимо:

1. Изменить пароль.
2. Проверить систему на наличие вирусов с помощью антивирусной программы.
3. Проверить, были ли установлены какие-либо сторонние программы, и удалить их.

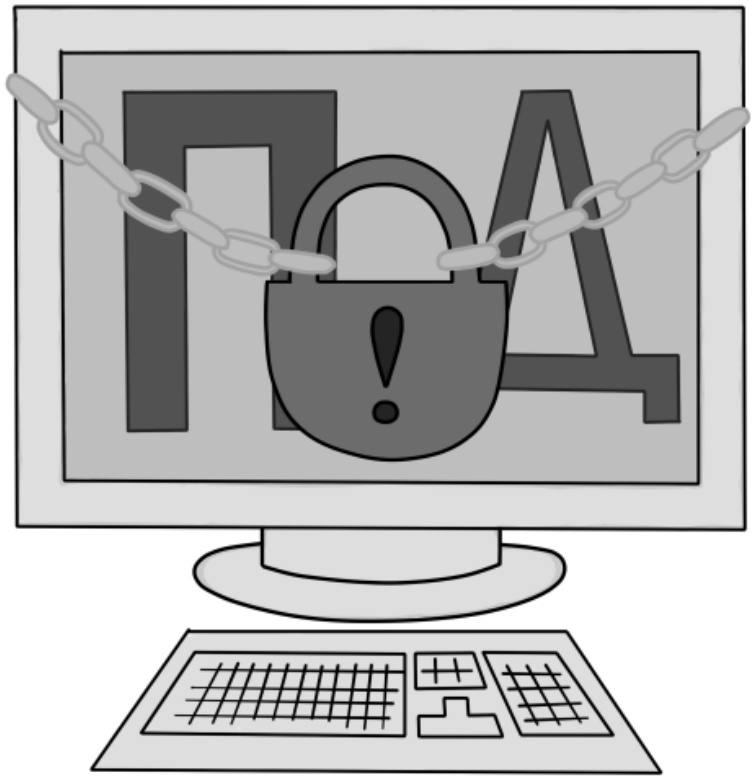
В случае повреждения личных файлов или файлов ОС необходимо:

1. Восстановить файлы с помощью резервных копий.
2. Проверить систему на наличие вирусов с помощью антивирусной программы.

Немаловажным фактором в работе системы защиты информации является периодическое сканирование компьютера антивирусными программами.

Таким образом, мы создали СЗИ, которая учитывает основные угрозы для домашнего компьютера; содержит рекомендации по использованию средств защиты, чтобы снизить вероятность осуществления перечисленных угроз, а также информацию о затратах на реализацию данной СЗИ.

Будьте внимательны при работе за компьютером и берегите свои персональные данные!



Учебное издание

Алдарова Динара Андреевна
Глушкова Елена Максимовна
Иванов Александр Дмитриевич
Юшков Алексей Анатольевич

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ ДЛЯ ШКОЛЬНИКОВ И РОДИТЕЛЕЙ

Учебное пособие

Редактор *Л. А. Богданова*
Компьютерная верстка *О. Г. Пенский*

Подписано в печать 26.12.2018 Формат 60×84/16.
Усл. печ. л. 4,65. Тираж 100 экз. Заказ 3

Издательский центр
Пермского государственного
национального исследовательского университета.
614990, г. Пермь, ул. Букирева, 15

Отпечатано: ООО «Ризо-Эксперт».
614990, г. Пермь, ул. Героев Хасана, 9, оф. 10