УТВЕРЖДЕН
приказом ЦДТ «Хибины»
от 31.08.2018 № 285

РЕГЛАМЕНТ
по запуску и обновлению антивирусного программного обеспечения

1. Основные положения

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 па:

— *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 вебресурс.

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 па 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 карг, 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.

Интернет - 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 - 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.

2. Компьютерные вирусы и их классификация

Компьютерный вирус – вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в другие программы (исполняемые файлы), документы, загрузочные сектора носителей данных.

Одним из способов классификации компьютерных вирусов – это разделение их по следующим основным признакам:

- среда обитания;
- особенности алгоритма проникновения в ПК;
- способы заражения;
- степень воздействия (безвредные, опасные, очень опасные).

В зависимости от среды обитания основными типами компьютерных вирусов являются:

- программные (поражают файлы с расширением COM или EXE) вирусы.
- Загрузочные вирусы;
- Макровирусы;
- Сетевые вирусы.

Программные вирусы – это вредоносный программный код, который внедрен внутрь исполняемых файлов (программ). Вирусный код может воспроизводить себя в теле других программ – этот процесс называется размножением. Создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удаляя информацию, хранящуюся на жёстком диске. Этот процесс называется вирусной атакой.

Загрузочные файлы – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков).

Макровирусы – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

Сетевые вирусы пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

3. Виды угроз

По алгоритмам работы различают компьютерные вирусы:

3.1.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).

3.2. 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.*

3.3. 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.

3.4. 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.

3.5. 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:

S отслеживание действий пользователя на компьютере;

S 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;

S сбор информации о качестве связи, способе подключения, скорости модема и т.д.

3.6. 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.

3.7. 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.

3.8. 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.

3.9. 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 - 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 - 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.

Снам - 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.

4. Основные требования по защите информации от компьютерных вирусов

Одним из основных способов борьбы с вирусами является своевременная профилактика.

Чтобы предотвратить заражение вирусами, необходимо следовать требованиям:

- не скачивать программы из интернета без проверки на наличие в них вируса;
- не открывать вложенные файлы (документы) в сообщениях, полученных от неизвестных адресатов;
- не открывать вложенные файлы (документы) в сообщениях от знакомых, если характер содержимого точно не известен. Отправитель может и не подозревать о наличии вируса в сообщении.
- Не открывать никогда вложенные файлы с типом exe – это запускаемые на выполнение программы;
- Иметь копии всех созданных важных документов на съемном носителе информации, так как восстановить информацию после заражения чаще всего невозможно;
- Необходимо регулярно проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать их содержимое;
- Необходимо пользоваться антивирусной программой, установленной на компьютере: оперативно (как минимум – три раза в неделю) выполнять обновление баз данных антивирусной программы;
- регулярно (как минимум- один раз в неделю) сканировать жесткие диски и съемные носители на обнаружение вирусов.
- Незамедлительно сообщать о заражении директору ЦДТ «Хибины».
- Помнить, что основное средство защиты информации – это резервное копирование ценных данных.

5. Признаки заражения компьютера

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

6 . Описание работы антивирусного программного обеспечения

На все компьютерах ЦДТ «Хибины» установлено лицензионное антивирусное программное обеспечение

Программное обеспечение состоит из следующих компонентов:

- файловый Антивирус – компонент, контролирующих файловую систему компьютера, Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере;

- почтовый Антивирус – компонент проверки всех входящих и исходящих почтовых сообщений компьютера;

- веб-Антивирус – компонент, который перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу;

Основные задачи программного обеспечения – защита от вредоносных программ, работа сетевого экрана и системы предотвращения вторжений.

Для выполнения этих задач в антивирусе реализованы функции:

1. Эвристический анализ. Это технология обнаружения угроз, не определяемых с помощью антивирусных баз. Она позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного. Анализатор включает поиск в коде подозреваемых признаков, характерных для вредоносных программ.

Файлы, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными.

2. Проективная защита. Основана на контроле и анализе поведения всех программ, установленных на компьютере. На основании выполняемых действий программное обеспечение принимает решение: является программа опасной или нет. Таким образом, компьютер остается защищенным не только от уже известных вирусов, но и от новых, еще не исследованных.

К опасному или вредоносному поведению программного обеспечения может относиться следующая активность:

- активность, характерная для троянских программ;

допуск к ресурсам (например, к реестру системы);

- самокопирование программы на сетевые ресурсы, в каталог автозапуска, в системный реестр с последующей рассылкой своих копий;
- перехват ввода данных с клавиатуры;
- скрытая установка драйверов;

Все вышеперечисленные виды активности контролируются и анализируются программным обеспечением с тем, чтобы оградить компьютер от известных, неизвестных и комплексных угроз.

3. Мониторинг системы обнаруживает и анализирует подозрительную активность на рабочих станциях. Он помогает защитится от новых угроз, которые еще не попали в базу сигнатур. Если вредоносная программа нарушает работу операционной системы, вносит изменения в системный реестр или важные файлы, то благодаря отслеживанию действий Мониторингом системы можно выполнить откат вредоносных действий.

4. Система предотвращения вторжений. Действия некоторых приложений, которые не являются вредоносными, могут расцениваться как представляющие серьезную угрозу. Во многих случаях рекомендуется запретить такие действия. Функция предотвращения вторжений ограничивает действия, выполняемые на конечном устройстве, соблюдая уровень доверия, назначенный приложению. Система работает вместе с персональным сетевым экраном на уровне приложений, которые ограничивают действия в сети.

5. Защита от сетевых атак служит для отслеживания подозрительной сетевой активности. При обнаружении подозрительного поведения решение реагирует согласно заранее заданным правилам.

6. Контроль программ. Инструменты контроля программ, разработанные программным обеспечением позволяют вести списки приложений.

7. Контроль устройств. Инструменты контроля устройств позволяют легко определить устройства, которым разрешается доступ в корпоративную сеть. Можно настроить ограничения по времени суток, географическому расположению или типу

устройства.

8. Веб-Контроль позволяет настроить политику доступа в интернет и контролировать его использование.

7. 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:

1 .Безотлагательно установите антивирусную программу.

2. Регулярно обновляйте сигнатуры угроз, входящие в состав программы.

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

1. Проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-карты и пр.) перед их использованием.

2.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.

3. Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо вебсайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.

4. Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью антивирусной программы.

5. 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-.*

1 .Своевременно делайте резервное копирование данных.

2. 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/удалеиие программ** в **Панели инструментов** или просто просмотреть содержимое каталога **Program Files,** каталога автозагрузки.

Основные антивирусные программы:

1. Microsoft Security Essentials
2. Windows Defender
3. Norton Antivirus
4. Dr. Web
5. Kaspersky Antivirus
6. NOD 32
7. Panda Antivirus