**Тема 3-4 Современные компьютерные угрозы и методы борьбы с ними**

**Цель:** Изучить существующие компьютерные угрозы и основные методы противодействия угрозам

**Вопросы практического занятия:**

*Компьютерные вирусы. Классификация компьютерных вирусов. Методы построения и внедрения шпионов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов и вредоносные программные средства. Устройство, принципы внедрения и действий компьютерных вирусов и вредоносных программных средств.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы. Обоснуйте свои ответы.

3 Дискуссия на темы(устный доклад):

5.1 Типы шпионов. Отличие от «классических» вирусов.

5.2 Жизненный цикл шпиона.

5.3 Методы построения и внедрения шпионов.

5.4 Обзор некоторых представителей шпионского ПО.

**5.5 Методы борьбы со шпионами. Пример anti spyware.**

**Контрольные вопросы:**

1. Что могут заразить вирусы?

Ответ:

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах.

**2. Как маскируются «невидимые» вирусы?**

Ответ:

Многие резидентные вирусы (и файловые, и загрузочные) предотвращают своё обнаружение тем, перехватывают обращения операционной системы (и тем самым прикладных программ) к заражённым файлам и областям диска и выдают их в исходном (незаражённом) виде. Такие вирусы называются невидимыми, или stealth (стелс) вирусами. Разумеется, эффект «невидимости» наблюдается только на заражённом компьютере – на «чистом» компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

**3. Каковы особенности самомодифицирующихся вирусов?**

Ответ:

Самомодифицирующиеся вирусы. Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.

**4. Какие методы защиты от компьютерных вирусов можно использовать?**

**Использование приложения для** защиты от вредоносных программ. Установка и обновление вредоносных программ поможет защитить компьютер от вирусов и других вредоносных программ.   
  
В Microsoft Defender есть бесплатное антивредоносное программное обеспечение, которое входит в Windows и автоматически обновляется с помощью Windows Обновления. Существуют также антивирусные продукты, которые можно выбрать из других компаний.

Одновредное запуск нескольких приложений для защиты от вредоносных программ может привести к медленному или нестабильному работе системы. Если вы установите антивредоносное приложение из другой компании, Microsoft Defender автоматически отключит себя. Однако при установке двух приложений, работающих с вредоносными программами других компаний, они могут попытаться запустить их одновременно.

* **Не открывайте сообщения электронной почты от незнакомых отправителей или незнакомые вложения**. Многие вирусы передаются в виде вложений в электронные письма, и для их распространения достаточно открыть вложение. Настоятельно рекомендуем открывать только ожидаемые или известные вам вложения. Дополнительные сведения см. в следующем разделе: [Защита от фишинга.](https://support.microsoft.com/ru-ru/windows/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BE%D1%82-%D1%84%D0%B8%D1%88%D0%B8%D0%BD%D0%B3%D0%B0-0c7ea947-ba98-3bd9-7184-430e1f860a44)
* **Блокируют всплывающие** окна в веб-браузере. Всплывающие окна — это небольшие окна браузера, которые отображаются в верхней части просматриваемого веб-сайта. Несмотря на то, что большинство таких окон используется для рекламных целей, в них может содержаться вредоносный или небезопасный код. Блокирование всплывающих окон позволяет избавиться от некоторых или даже всех всплывающих окон. Блокирование всплывающих окон в Microsoft Edge включено по умолчанию.
* **При использовании Microsoft Edge, убедитесь, что SmartScreen включен**. SmartScreen в Microsoft Edge помогает защитить от фишинга и атак вредоносных программ, предупреждая о возможной небезопасности веб-сайта или расположения загрузки. Дополнительные сведения см. в разделе [Что такое фильтр SmartScreen и как он меня защищает?](https://support.microsoft.com/ru-ru/microsoft-edge/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80-smartscreen-%D0%B8-%D0%BA%D0%B0%D0%BA-%D0%BE%D0%BD-%D0%BC%D0%B5%D0%BD%D1%8F-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B0%D0%B5%D1%82-1c9a874a-6826-be5e-45b1-67fa445a74c8)
* **Обратите внимание на уведомления Windows SmartScreen**. С осторожностью запускайте неизвестные приложения, скачанные из Интернета. Такие приложения с большой вероятностью могут оказаться небезопасными. Когда вы скачиваете и запустите приложение из Интернета, SmartScreen использует сведения о репутации приложения, чтобы предупреждать вас, если приложение не известно и может быть вредоносным.
* **Регулярно обновляйте Windows**. Корпорация Майкрософт регулярно выпускает особые обновления для системы безопасности, предназначенные для защиты компьютера. Обновления могут предотвратить атаки вирусов и других вредоносных программ, закрывая возможные слабые места в системе безопасности.  
    
  Windows Обновление позволяет убедиться в том, что компьютер получает эти обновления автоматически, но иногда может потребоваться периодически перезапускать компьютер, чтобы полностью установить обновления.
* **Используйте параметры** конфиденциальности браузера. Некоторые веб-сайты могут пытаться использовать ваши персональные данные для целевой рекламы, мошенничества и кражи личных данных. Во всех современных браузерах есть параметры конфиденциальности, которые можно включить для управления тем, какие сайты могут видеть и делать.  
    
  Дополнительные сведения о настройке параметров конфиденциальности в Microsoft Edge см. в разделе [Настройка параметров конфиденциальности согласно вашим потребностям.](https://support.microsoft.com/ru-ru/microsoft-edge/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0-%D0%BF%D0%B0%D1%80%D0%B0%D0%BC%D0%B5%D1%82%D1%80%D0%BE%D0%B2-%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D1%81%D0%BE%D0%B3%D0%BB%D0%B0%D1%81%D0%BD%D0%BE-%D0%B2%D0%B0%D1%88%D0%B8%D0%BC-%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BD%D0%BE%D1%81%D1%82%D1%8F%D0%BC-8c923c9d-4ef2-849d-a399-4de716ecbbaf)
* **Убедитесь, что функция контроля учетных записей включена**. При внесении на компьютере изменений, требующих прав администратора, функция контроля учетных записей уведомит вас об этом и предложит утвердить эти изменения. Контроль учетных записей не позволяет вирусам вносить нежелательные изменения. Чтобы открыть контроль учетных записей, проведите пальцем от правой границы экрана, а затем коснитесь элемента **Поиск**. (Если вы используете мышь, наведите указатель на правый верхний угол экрана, переместите указатель вниз, а затем щелкните **Поиск**.) Введите в поле поиска **контроль учетных записей**, а затем выберите элемент **Изменение параметров контроля учетных записей**.
* **Убедитесь,** что защита тамперов включена. В Windows 10 и 11 есть функция Подделывка, которая предотвращает изменение параметров безопасности несанкционированными приложениями. Многие вирусы и вредоносные программы пытаются отключить антивирусную программу или другие параметры безопасности при их установке, чтобы избежать обнаружения. Сведения [о том,](https://support.microsoft.com/ru-ru/topic/%D0%B7%D0%B0%D0%BF%D1%80%D0%B5%D1%82-%D0%BD%D0%B0-%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D0%B0%D1%80%D0%B0%D0%BC%D0%B5%D1%82%D1%80%D0%BE%D0%B2-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D1%81-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%BE%D0%B9-%D0%BE%D1%82-%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D0%BB%D0%BA%D0%B8-6fd8d8ff-0e6d-4df5-b994-ea4df20ca969) как это сделать, см. в сведениях о том, как это сделать, см. в сведениях о том, как запретить изменение параметров безопасности с помощью защиты от подстановки.

**5. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?**

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать: общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя; профилактические меры, позволяющие уменьшить вероятность заражения вирусом; специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов.

Имеются две основные разновидности этих средств: копирование информации - создание копий файлов и системных областей дисков; разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины

(иммунизаторы).

**6. На какие виды можно подразделить программы защиты от компьютерных вирусов?**

Во-первых, антивирусы можно подразделить на две категории:

программы, которые непрерывно сканируют потоки данных, например, интернет-трафика, принудительно запускаемые программы с целью сканирования определенных, указанных объектов.

Во-вторых, антивирусные программы различаются по виду (способу) защиты от вирусов. Тут можно выделить следующие: Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса. Программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus. Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей. Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас". Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

**7. Как действуют программы-детекторы?**

Детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ. Многие программы-детекторы позволяют также «лечить» зараженные файлы или диски, удаляя из них вирусы (разумеется, лечение поддерживается только для вирусов, известных программе-детектору). Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов

Программы детекторы

Aidstest

Doctor Web

MicroSoft AntiVirus

другие

**8. Что называется сигнатурой?**

Сигнатура функции — часть общего объявления функции, позволяющая средствам трансляции идентифицировать функцию среди других. В различных языках программирования существуют разные представления о сигнатуре функции, что также тесно связано с возможностями перегрузки функций в этих языках.

Иногда различают сигнатуру вызова и сигнатуру реализации функции. Сигнатура вызова обычно составляется по синтаксической конструкции вызова функции с учётом сигнатуры области видимости данной функции, имени функции, последовательности фактических типов аргументов в вызове и типе результата. В сигнатуре реализации обычно участвуют некоторые элементы из синтаксической конструкции объявления функции: спецификатор области видимости функции, её имя и последовательность формальных типов аргументов.

Например, в языке программирования C++ простая функция однозначно опознаётся компилятором по своему имени и последовательности типов своих аргументов, что составляет сигнатуру функции в этом языке. Если функция является методом некоторого класса, то в сигнатуре будет участвовать и имя класса.

В языке программирования Java сигнатуру метода составляют его имя и последовательность типов параметров; тип возвращаемого значения в сигнатуре не участвует.

**9. Всегда ли детектор распознает зараженную программу?**

**Программы-детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется **сигнатурой**. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

**10. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?**

**Программа**-**ревизоры** относятся к самым надежным средствам защиты от вирусов. **Ревизоры** запоминают исходное состояние **программ**, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным.

**11.Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?**

Первый уровень защиты – это внимательность и информирование пользователей.

В прошлом году количество хакерских атак выросло на 50%, увеличивая вероятность рисков на предприятиях. К тому же, по данным 2015 года - у каждого четвертого интернет-пользователя в странах ЕС, возникали проблемы, связанные с безопасностью. Для обеспечения надежности бизнеса в будущем, вопросы безопасности уже сегодня на повестке дня любого предприятия.

Международное распространение в последнее время получили такие вирусы-вымогатели как Wannacry, Petya, NotPetya, Schrodinger’s Petya, а также Misha, хотя они не являются новой угрозой для общества, ведь разновидности таких вирусов появились еще в 2005 году. Распространение вирусов-вымогателей происходит весьма просто, как правило по невнимательности пользователей и как следствие доверия источнику, ведь э-майл может прийти от знакомого отправителя. Получая такой э-майл с инфицированным приложением, пользователь активизирует работу вируса всего одним кликом. Далее вирус крадет доступ к системе пользователя, используя память компьютера, и пытается распространиться уже по локальной сети, впоследствии распространяясь по интернету.

Регулярные обучения по вопросам безопасности на предприятии, в том числе, информирование сотрудников о потенциальных угрозах при работе с электронной почтой не требует дополнительных расходов, зато поможет предотвратить угрозу.

Второй уровень – это защита рабочего компьютера.

Согласно статистике - 1 из 131 полученного э-майла является инфицированными вирусом, однако многие пользователи их даже не получают, так как установленные программы для фильтрации сообщений и антивирус автоматически производят отбор и блокируют подозрительные. Такие инструменты широко распространены и наряду с последними обновлениями операционной системы (ОС) служат так называемой защитой второго уровня.

В мае этого года многие пользователи пострадали от одной из самых массовых кибер-атак всего лишь по той причине, что на их компьютерах не было установлено последнее обновление операционной системы Майкрософт, которое бы не позволило вирусу распространиться дальше. При таком развитии разновидностей вирусов обновление ОС все же позволяет остановить их работу, по крайней мере частично.

Третий уровень - это превентивные меры или план по защите бизнеса.

Как действовать руководителю предприятия, ИТ-специалисту или продавцу компании в случае распространения вируса? Что происходит с хранением данных в облаке или на сервере, продолжают ли они работать и находиться в безопасности?

Положительной практикой на предприятии считается надежное хранение и обработка конфиденциальных и других важных бизнес-данных. Разумно создавать продуманный [план аварийного восстановления предприятия](https://www.deac.eu/reshenia/rieshieniia-dlia-zashchity-dannykh/plan-avariinogho-vosstanovlieniia/plan-avariinogho-vosstanovlieniia/ru/?utm_source=forum-ru&utm_campaign=deac-protection) (ПАВ или Disaster Recovery Plan), который обеспечит непрерывность бизнес-процессов и предотвратит потенциальные простои. Для каждого предприятия такой план будет отличаться, однако главной ценность такого плана – полученный определенный промежуток времени, в течение которого все ИТ-системы компании восстановятся и вернутся в рабочий режим.

Предприятие может самостоятельно подготовить план аварийного восстановления или же использовать услуги ИТ-аутсорсинга в дата-центре, доверив эту функцию сертифицированным специалистам, которые не только разработают комплекс действий, но и обеспечат необходимый мониторинг систем. Также, в случае непредвиденных обстоятельств, ИТ-эксперты помогут возобновить рабочие процессы.

Четвертый уровень – это комплексные решения для 100% безопасности.

Если вирус все-таки попал в рабочую среду пользователя и распространяется в локальной сети, как предотвратить простои, финансовые потери и оперативно восстановить работу бизнеса? На рынке кибер-защиты доступны различные решения или *вакцины*, которые могут частично расшифровать инфицированные компьютеры. Однако доступ к таким услугам ограничен и не всегда применим из-за различий вирусных программ.

Следовательно, правильней действовать наперед - оценить критически важные бизнес-процессы и диверсифицировать риски с помощью [комплексных решений](https://www.deac.eu/reshenia/rieshieniia-dlia-zashchity-dannykh/rieshieniia-dlia-zashchity-dannykh/ru/?utm_source=forum-ru&utm_campaign=deac-protection). Это позволяет предвидеть потенциальные риски, а также быстро и эффективно предотвратить критическую ситуацию. Даже в случае инфицирования вирусом, данные могут быть защищены, и рабочая среда восстановлена в кратчайшие сроки с помощью доступных профилактических методов. Однако способы защиты будут зависеть от используемого предприятием ИТ-оборудования:

* Предприятиям, которые в работе используют персональные компьютеры (ПК), рекомендуется воспользоваться услугой удаленного доступа (Desktop as a Service), которая обеспечит надежную работу с данными из любого места. По сути, это тот же рабочий стол компьютера со всеми программами и данными, только данные не хранятся на ПК, а находятся на сервере в дата-центре. Услугу удаленного доступа лучше всего использовать в комбинации с [резервным копированием данных](https://www.deac.eu/reshenia/rieshieniia-dlia-zashchity-dannykh/baas/rieziervnoie-kopirovaniie-dannykh/ru/?utm_source=forum-en&utm_campaign=deac-protection#1) (Back up as a Service), так как резервные копии — это простой и эффективный способ, как восстановить данные в течении часа. Предприятие может самостоятельно решить, как часто и в каком объеме им необходимо создавать резервные копии и кому из сотрудников предоставлять доступ к таким данным. Но важно отметить, что для большей безопасности копии необходимо создавать и хранить в дата-центрах по крайней мере с двумя разными локациями, идеально - в разных странах с различной юрисдикцией.
* В свою очередь, предприятиям, которые используют [выделенные](https://www.deac.eu/reshenia/arenda-serverov/vydieliennyie-sierviery/vydieliennyie-sierviery/ru/?utm_source=forum-ru&utm_campaign=deac-protection#1), [виртуальные серверы](https://www.deac.eu/reshenia/oblachnie-uslugi/virtualnyie-sierviery/virtualnyie-sierviery/ru/?utm_source=forum-en&utm_campaign=deac-protection#1) или [частное облако](https://www.deac.eu/reshenia/oblachnie-uslugi/chastnoie-oblako/oblako/ru/?utm_source=forum-ru&utm_campaign=deac-protection), желательно застраховаться с помощью уже упомянутого резервного копирования данных и плана аварийного восстановления, который поможет восстановить данные даже через 15-30 минут. Важный аспект при выборе дата-центра - возможность предоставить индивидуальные решения по защите данных. Ведь восстановление может потребоваться не только данным, но и приложениям. Особое внимание стоит уделить используемой программе по обеспечению резервного копирования. Она должна быть не только достаточно эластичной для репликации системы данных всего предприятия, но и иметь возможность восстановления в максимально короткие строки, не допуская остановку работы предприятия. Одна из самых распространённых программ такого рода является Veeam, которую операторы дата-центров предоставляют в комплексе с различными решениями по обработке и хранению данных.

**12. Перечислите меры защиты информации от компьютерных вирусов.**

Для защиты от вирусов можно использовать:

· общие средства защиты информации – страховку от физиче­ской порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

· профилактические меры, позволяющие уменьшить вероят­ность заражения вирусом;

· специализированные программы для защиты от вирусов.

Общие средства зашиты информации необходимы не только для защиты от вирусов. Имеются две основные разновидности этих средств:

· средства резервного копирования информации – создание копий файлов и системных областей дисков;

· средства разграничения доступа – предотвращают несанкцио­нированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами, а также ошибочные действия пользователей.

Несмотря на то, что общие средства защиты информации очень важны, их одних для защиты от вирусов все же недостаточно. По­этому для защиты от вирусов необходимо применять специализи­рованные программ

**13. Каковы современные технологии антивирусной защиты?**

Самая распространенная антивирусная технология, предназначенная для выявления неизвестных типов кибер-угроз, - это метод эвристического анализа, на основе которого сегодня функционируют многие программы, например, бесплатный антивирус Avast. Суть этой технологии заключается в том, что для обнаружения вируса используется компонент «безопасная среда», то есть зловред запускается в защищенной области, при этом его действия анализируются искусственным интеллектом. Такие возможности антивируса пользователь сможет ощутить на примере установленной у себя ОС, если решит, например, скачать kaspersky.

Еще одна популярная современная антивирусная технология — это поведенческие блокираторы, которые являются основным модулем большинства современных защитных программ. Этот принцип используется, как правило, в профессиональных антивирусных продуктах вроде «Антивируса Касперского» и Dr.Web'а, однако он отсутствует в небольших утилитах вроде программы Cureit. Блокираторы предназначены для постоянного контроля над системой и всеми установленными на компьютере приложениями. При этом такой компонент чаще всего оснащен модулем самообучения — таким образом достигается его наибольшая эффективность.

Инспекторы изменений — это еще один способ выявления вирусов, который, однако, используется намного реже блокираторов и метода эвристики. Инспекторы хранят в отдельной базе данные обо всех имеющихся на компьютере файлах и время от времени осуществляют проверку на наличие в них изменений. В случае присутствия стороннего кода антивирус проводит его тщательное сканирование, а затем предлагает пользователю вылечить или удалить зараженные файлы.