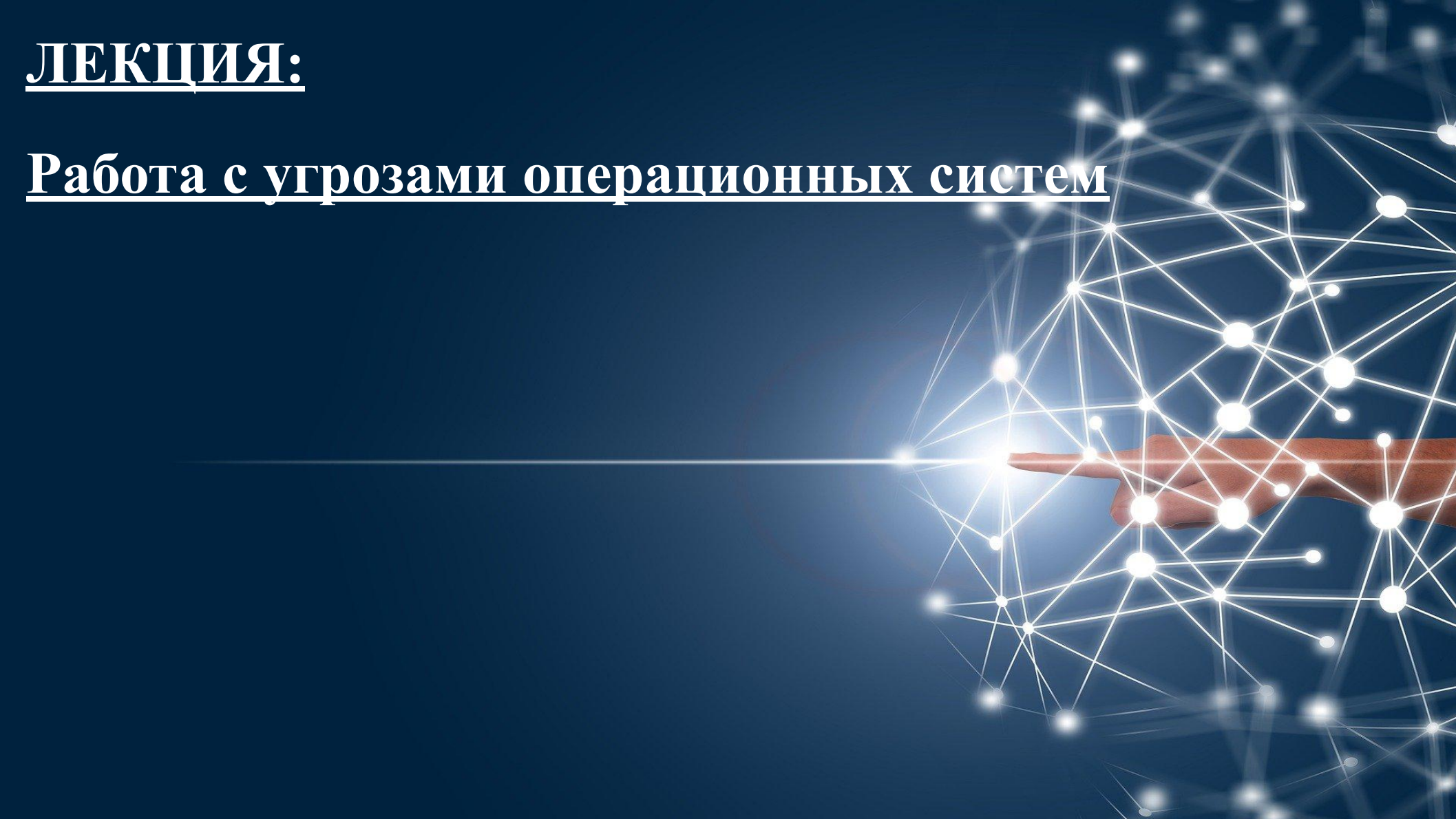
ЛЕКЦИЯ:

Работа с угрозами операционных систем



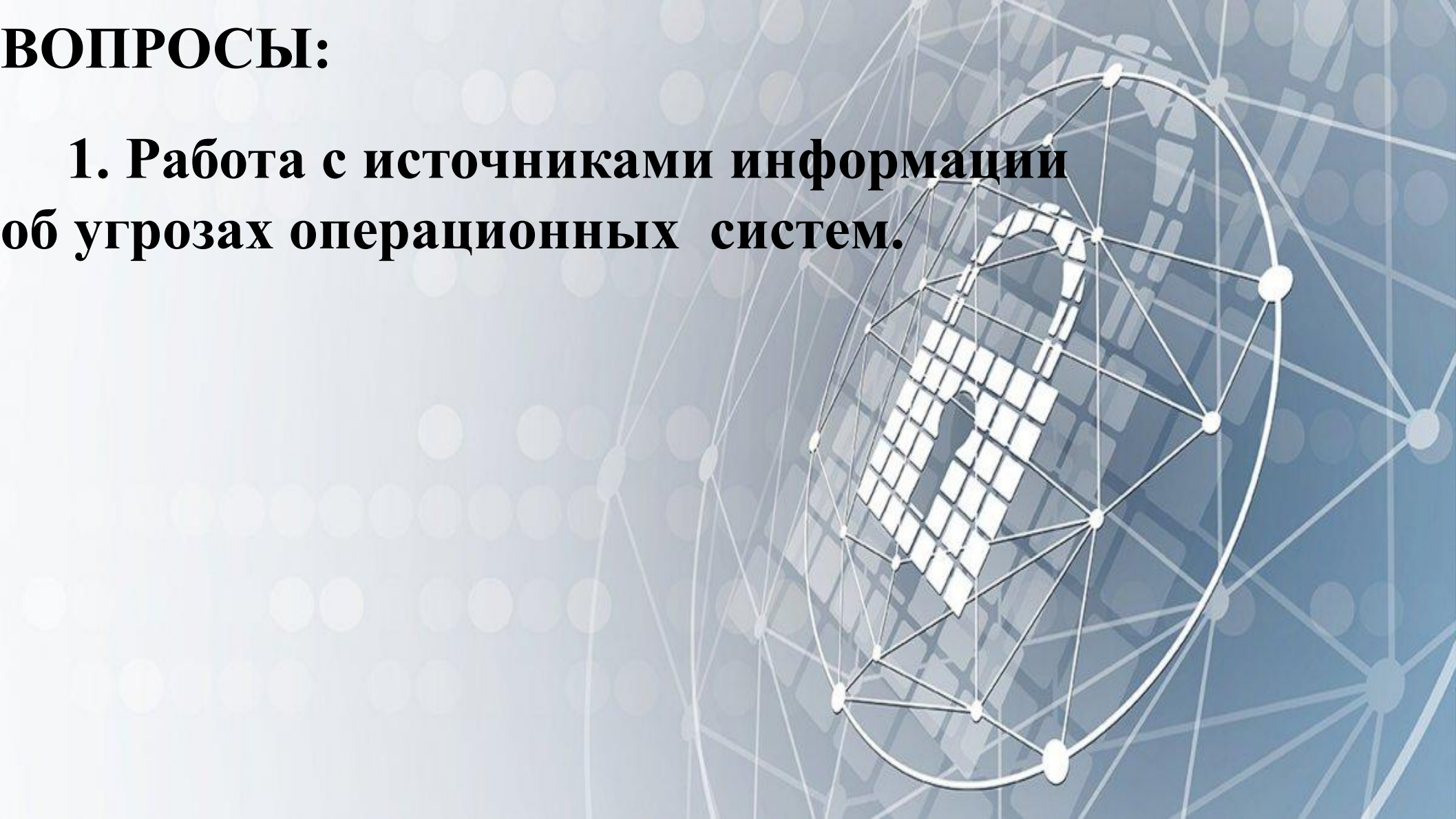
ВОПРОСЫ:

1. Работа с источниками информации об угрозах операционных систем.

2. Работа по локализации угроз операционных систем.

ВОПРОСЫ:

1. Работа с источниками информации об угрозах операционных систем.



Работа с источниками информации об угрозах операционных систем.

CASE

"Хакеры легко взламывают Windows 10 — Microsoft пока бессильна"

Злоумышленники создают файлы Microsoft Office, которые открывают им доступ к системе. К счастью, можно перекрыть доступ, отключив опасную функцию.
Хакеры обнаружили в Windows 10 ранее неизвестную уязвимость и используют ее для взлома компьютеров.

Компания Microsoft предупредила пользователей об опасности и объяснила, как защититься, пока не выйдет официальный патч.

Уязвимостями нулевого дня (zero-day vulnerability) называют "лазейки" в операционной системе, которые злоумышленники находят раньше разработчиков. С их помощью хакеры могут удаленно запускать на компьютере вредоносные программы или перехватывать контроль. Новая уязвимость получила название **CVE-2021-40444**, о ней 5 сентября 2021 года сообщил исследователь с ником EXPMON.

Работа с источниками информации об угрозах операционных систем.

Проблема скрывается в механизме ***рендеринга браузера Internet Explorer — MSHTML***. Казалось бы, мало кто пользуется стандартным браузером Microsoft, однако этот механизм также используют ***программы Microsoft Office с расширением "docx". Хакеры могут встраивать в них вредоносный элемент управления ActiveX (фреймворк для определения программных компонентов), который будет использовать документ с механизмом визуализации Internet Explorer.***

Как только открывается такой файл — начинается взлом системы. Пользователи с правами администратора рискуют пострадать сильнее, чем обладатели учетных записей с низким уровнем доступа. По словам разработчиков, антивирус Microsoft Defender может обнаруживать вмешательство, однако полностью от атак не защищает. Патч ожидается только, 14 сентября 2021 года.

«Классификация угроз операционных систем.»

Классификация типичных атак:

Сканирование файловой системы. Злоумышленник просматривает файловую систему компьютера и пытается прочитать (скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, которая должна быть ему запрещена;

«Классификация угроз операционных систем.»

Классификация типичных атак:

Угадывание пароля. Есть несколько методов подбора паролей пользователей:

- тотальный поиск;
- брутфорс, оптимизированный по статистике появления символов или с помощью словарей;
- подбор пароля с учетом знаний о пользователе (его имя, фамилия, дата рождения, номер телефона и т. д.).

«Классификация угроз операционных систем.»

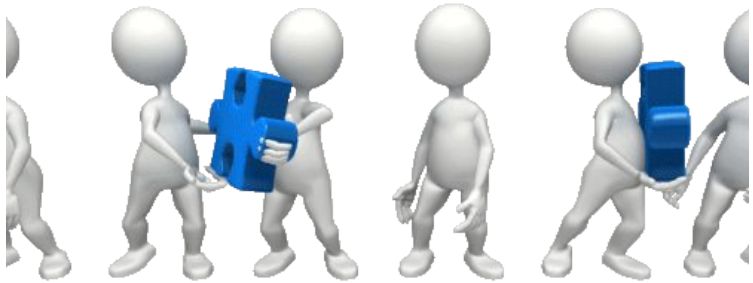
Классификация типичных атак:

Кража ключевой информации. Злоумышленник может следить за паролем, введенным пользователем, или восстанавливать введенный пароль, перемещая руки по клавиатуре. Можно просто украсть.

«Классификация угроз операционных систем.»

Классификация типичных атак:

Сборка мусора. Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Злоумышленник восстанавливает эту информацию, просматривает и копирует интересующие его фрагменты.



«Классификация угроз операционных систем.»

Классификация типичных атак:

Злоупотребление властью. Злоумышленник, использующий ошибки в рейтинге программного обеспечения ОС или политике безопасности, имеет полномочия, превышающие полномочия, предоставленные ему в соответствии с политикой безопасности. Обычно это достигается запуском программы от имени другого пользователя.

«Классификация угроз операционных систем.»

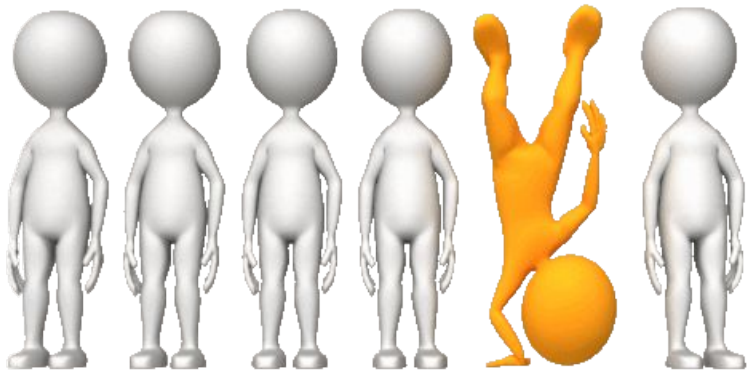
Классификация типичных атак:

Закладки программы. Программные закладки, встроенные в ОС, программно не отличаются от закладок других кл[illegible].

«Классификация угроз операционных систем.»

Классификация типичных атак:

Жадные программы — это программы, которые намеренно потребляют большие ресурсы компьютера, чтобы создать медленную работу других программ. Запуск жадной программы может привести к сбою ОС.



Работа с источниками информации об угрозах операционных систем.

- Мониторинг существования известных уязвимостей:
  - мониторинг уязвимостей на официальных сайтах вендоров;
  - мониторинг специализированных публичных ресурсов;
  - **взаимодействие с CERT.BY.**

Работа с источниками информации об угрозах операционных систем.

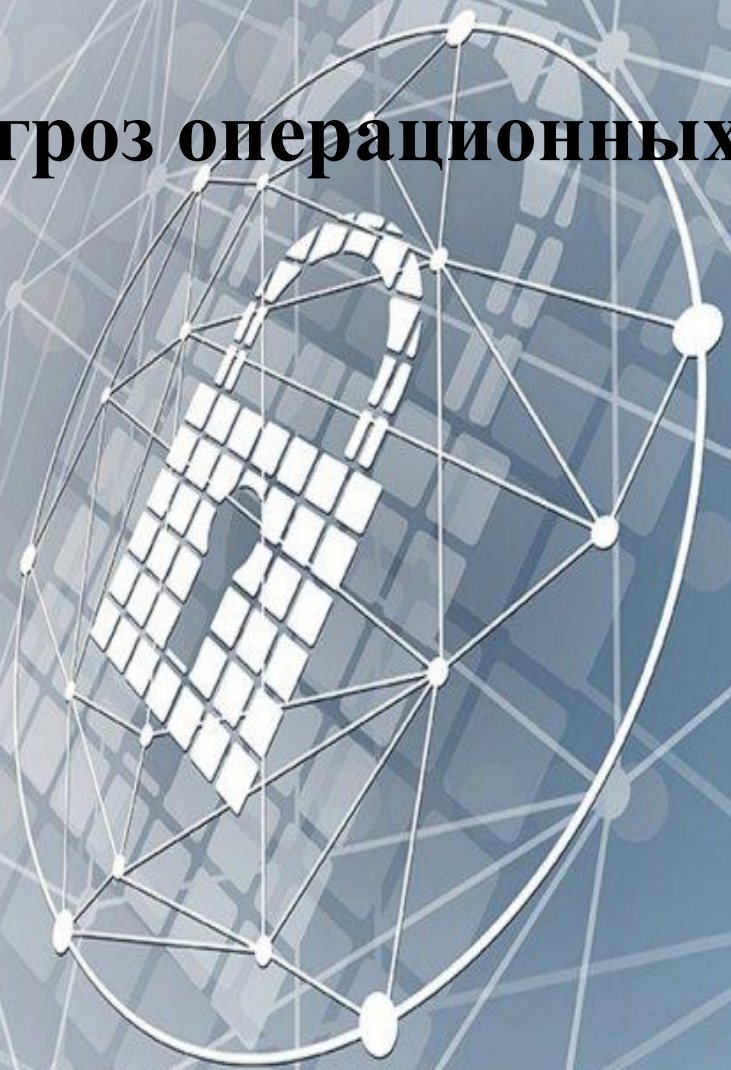
Мониторинг существования известных уязвимостей:

- мониторинг уязвимостей на официальных сайтах вендоров;
- мониторинг специализированных публичных ресурсов:

https://cve.mitre.org;
https://nvd.nist.gov;
https://cvedetails.com;
https://www.cve.org;
https://www.exploit-db.com.

ВОПРОСЫ:

2. Работа по локализации угроз операционных систем.



Работа по локализации угроз операционных систем.

- ***Понятие защищенной операционной системы***

- **Операционную систему называют защищенной, если она предусматривает средствА защиты от основных классов угроз!** Защищенная операционная система обязательно должна содержать ***средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с операционной системой.*** Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.

Работа по локализации угроз операционных систем.

- **Понятие архитектуры подсистем защиты операционной системы.**

- ***Подсистема защиты ОС выполняет следующие основные функции:***

- **Идентификация и аутентификация.**
- Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Разграничение доступа.**
- Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Аудит.**
- Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Управление политикой безопасности.**
- Политика безопасности должна постоянно поддерживаться в адекватном состоянии, то есть должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в операционную систему, или установленных дополнительно для данной цели.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Криптографические функции.**
- Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Сетевые функции.**
- Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.

- ЗАЧЕМ ЭТО НАДО?

Работа по локализации угроз операционных систем.

- **Жизненный цикл ОС Windows. Виды поддержки.**
- Жизненный цикл каждой операционной системы начинается при выпуске продукта на рынок и заканчивается, когда ее поддержка прекращается. Знание основных дат жизненного цикла помогает в принятии решений о времени установки новой версии или внесении других изменений в используемые программы.
- Типичный жизненный цикл для ОС семейства Windows выглядит следующим образом:
- *Выпуск ОС.*
- *Основная поддержка (~5 лет).*
- *Расширенная поддержка (~5 лет).*
- *Окончание расширенной поддержки.*
- Строго говоря, жизненный цикл, операционной системы не заканчивается после окончания расширенной поддержки – она продолжит выполнять свои функции, вместе с тем мы настоятельно рекомендуем отказаться от использования устаревших версий ОС и перейти на более новую версию, не дожидаясь окончания периода расширенной поддержки.

Работа по локализации угроз операционных систем.

- **Жизненный цикл ОС Windows. Виды поддержки.**
- Жизненный цикл каждой операционной системы начинается при выпуске продукта на рынок и заканчивается, когда ее поддержка прекращается. Знание основных дат жизненного цикла помогает в принятии решений о времени установки новой версии или внесении других изменений в используемые программы.
- Типичный жизненный цикл для ОС семейства Windows выглядит следующим образом:
- *Выпуск ОС.*
- *Основная поддержка (~5 лет).*
- *Расширенная поддержка (~5 лет).*
- *Окончание расширенной поддержки.*
- Строго говоря, жизненный цикл, операционной системы не заканчивается после окончания расширенной поддержки – она продолжит выполнять свои функции, вместе с тем мы настоятельно рекомендуем отказаться от использования устаревших версий ОС и перейти на более новую версию, не дожидаясь окончания периода расширенной поддержки.

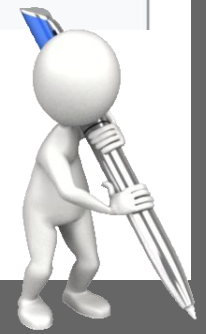
Работа по локализации угроз операционных систем.

- **Периоды (виды) поддержки ОС Windows**
- 1. ***Основная поддержка.*** Начинается с момента выхода ОС. Во время действия основной поддержки обращение пользователя по любым вопросам, связанным с функционированием ОС, рассматривается разработчиками, а ошибки устраняются. В данный период пользователю бесплатно доступны:
- *поддержка по инцидентам;*
- *поддержка исправлений, не связанных с безопасностью;*
- *обновления безопасности (обновления, закрывающие уязвимости, которые могут повлечь нарушение работы ОС);*
- *запрос на изменение вида и функций операционной системы.*
- 2. ***Расширенная поддержка.*** В отличие от основной поддержки разработчик бесплатно выпускает только обновления безопасности. Остальные виды поддержки можно получить за дополнительную плату.
- 3. ***Окончание периода расширенной поддержки.*** С этого момента прекращается выпуск обновлений безопасности, равно как и другие виды поддержки, ранее доступные пользователю. **Такая ОС становится уязвимой перед новым ВПО.** ***Кроме того, обновления безопасности, выпускаемые компанией производителем для устранения уязвимостей актуальных версий ОС (с действующей поддержкой), могут указать злоумышленнику на незащищенные места в устаревших ОС, и, тем самым, облегчить ему несанкционированный доступ к данным пользователя, который по какой-либо причине не актуализировал свою ОС.***

Работа по локализации угроз операционных систем.

- Согласно официальному сайту компании Microsoft, наиболее известные операционные системы семейства Windows имеют следующие периоды поддержки:

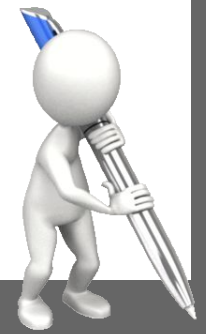
Операционная система	Окончание основной поддержки	Окончание расширенной поддержки
Windows XP	14 апреля 2009 г.	8 апреля 2014 г.
Windows Vista	10 апреля 2012 г.	11 апреля 2017 г.
Windows 7	13 января 2015 г.	14 января 2020 г.
Windows 8	9 января 2018 г. (выпуск обновлений до 12 января 2016 г.)	10 января 2023 г.
Windows 8.1	9 января 2018 г.	10 января 2023 г.
Windows 10	13 октября 2020 г.	14 октября 2025 г.

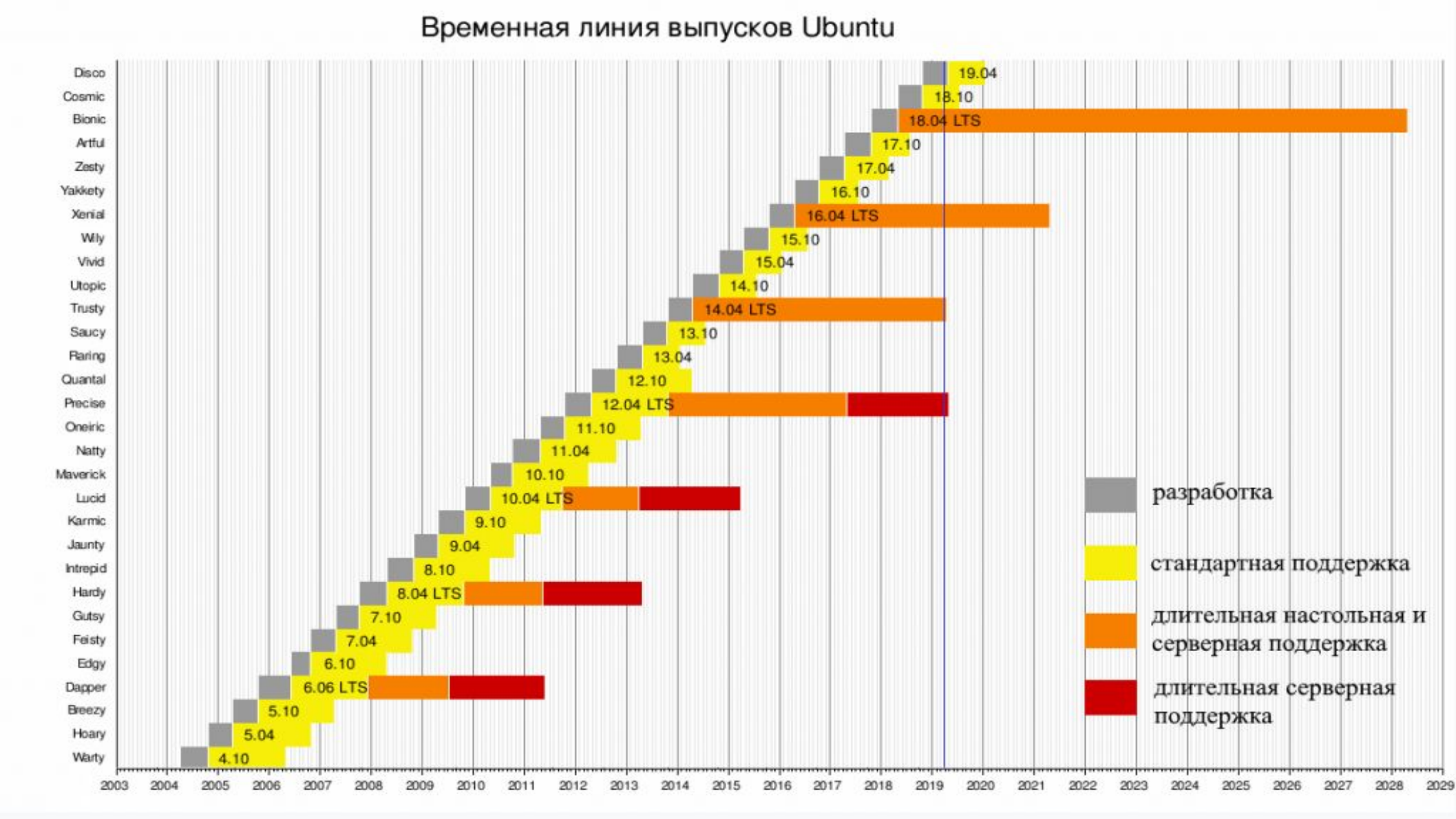


Работа по локализации угроз операционных систем.

Операционные системы семейства Linux

Linux – семейство операционных систем с открытым исходным кодом. То есть он доступен для просмотра, изучения и изменения, что позволяет убедиться в отсутствии уязвимостей или встроенного ВПО. Любой пользователь, обнаруживший уязвимость в ОС, может сообщить о ней разработчикам. Например, для популярной ОС Linux Ubuntu выпуском обновлений занимается британская компания Canonical.

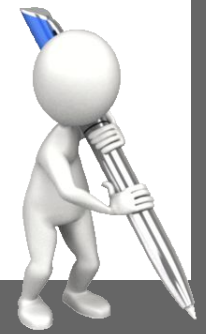



Временная линия выпусков Ubuntu
Disco
Cosmic
Bionic
Artful
Zesty
Yakkety
Xenial
Wily
Vivid
Utopic
Trusty
Saucy
Raring
Quantal
Precise
Oneiric
Natty
Maverick
Lucid
Karmic
Jaunty
Intrepid
Hardy
Gutsy
Feisty
Edgy
Dapper
Breezy
Hoary
Warty
19.04
18.10
18.04 LTS
17.10
17.04
16.10
16.04 LTS
15.10
15.04
14.10
14.04 LTS
13.10
13.04
12.10
12.04 LTS
11.10
11.04
10.10
10.04 LTS
9.10
9.04
8.10
8.04 LTS
7.10
7.04
6.10
6.06 LTS
5.10
5.04
4.10
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
разработка
стандартная поддержка
длительная настольная и серверная поддержка
длительная серверная поддержка

Работа по локализации угроз операционных систем.

Поскольку выпуск систем со стандартной поддержкой происходит каждые полгода, преимуществом таких версий является наличие современных программных решений и обновленного функционала. Недостаток же состоит в том, что после выпуска новой ОС возможны ошибки в ее работе, которые будут устраняться разработчиками.

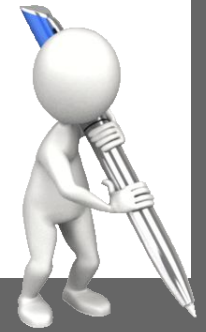
Для стабильной работы операционной системы и долгосрочного наличия поддержки, рекомендуется выбирать версию LTS!



Работа по локализации угроз операционных систем.

Список действующих ОС Linux Ubuntu с длительным периодом поддержки выглядит следующим образом:

Операционная система	Выпуск ОС	Окончание расширенной поддержки
Ubuntu 14.04 Trusty	17 апреля 2014 г.	17 апреля 2019 г.
Ubuntu 16.04 Xenial	21 апреля 2016 г.	21 апреля 2021 г.
Ubuntu 18.04 Bionic	26 апреля 2018 г.	26 апреля 2028 г.



СПАСИБО ЗА ВНИМАНИЕ!