Оглавление

[Безопасность в интернете 2](#_Toc150359823)

[Противостояние киберпреступникам. Виды киберпреступлений 3](#_Toc150359824)

[Масштабы распространения киберугроз и основные виды киберугроз 5](#_Toc150359825)

[Способы защиты от кибератак: советы по кибербезопасности 7](#_Toc150359826)

# Цифровые платформы как среда для решения проблем в эпоху цифрового общества

Расширение сферы применения цифровых технологий, доступность и распространенность цифровых устройств привели к формированию качественно новых условий, в которых становятся экономически осмысленными новые бизнес-модели, основанные на развитии цифровых экосистем, поддерживаемых цифровыми платформами. Цифровые платформы и экосистемы позволяют ускорить и удешевить доступ потребителей к товарам и услугам. Наиболее характерной особенностью цифровой экономики являются цифровые платформы.

Цифровые платформы – это автоматизированные информационные системы, позволяющие неограниченному кругу лиц использовать ее возможности через интернет для решения технологических и функциональных задач в автоматизированном режиме.

Обеспечивая взаимосвязь между участниками рынка, платформы рассматриваются в трех проекциях:

1. платформа как бизнес-модель (Платформа обеспечивает взаимосвязь между участниками рынка)
2. платформа как экосистема (потребители «осваивают» ценность, производимую другими участниками)
3. платформа как технология (платформа предоставляет уникальный интерфейс, который соединяет клиентов на разных сторонах)

Цифровые платформы принято классифицировать по различным признакам.

1. По степени развития предоставляемого функционала:
   1. технологические (предоставляют доступ к ИТ ресурсам и технологиям)
   2. функциональные (предоставляют доступ к специализированным инструментам)
   3. инфраструктурные (предоставляют доступ к цифровой инфраструктуре)
   4. корпоративные (оптимизируют процесс управления)
   5. информационные (предоставляют информационный доступ к рынку)
   6. маркетплейсы (предоставляют доступ к рынку, обеспечивая взаимодействие сторон)
   7. отраслевые (оптимизируют взаимодействия участников)
2. По характерным признакам цифровых платформ:
   1. инструментальные – основной вид деятельности на платформе связан с разработкой программных и программно- аппаратных решений, а результат – продукт (программное или программно-аппаратное средство) для обработки информации, как инструмент. Обеспечивают технологическую работу с данными, но не обеспечивают доступа к самим данным
   2. инфраструктурные – основной вид деятельности на платформе связан с предоставлением ИТ-сервисов и информации для принятия решений, а результат – ИТ-сервис и результат его работы – информация, необходимая для принятия решения в хозяйственной деятельности. Содержат в себе и средства технологической обработки данных, и источники данных, что позволяет в рамках соответствующих экосистем строить полезные в прикладном смысле ИТ-сервисы, насыщенные данными, необходимыми для принятия решений в рамках отдельного субъекта экономики
   3. прикладные – основной вид деятельности на платформе связан с обменом определёнными экономическими ценностями на заданных рынках, а результат – транзакция, сделка, фиксирующая обмен товарами/услугами между участниками на заданном рынке.

Отраслевая цифровая платформа рассматривается при этом как подтип прикладной цифровой платформы. Оперируют обработанными данными уже на уровне бизнес-процессов отдельной группы субъектов экономики или отрасли в целом.

# Аддитивные технологии. 3D-проектирование и печать. Принципы реализации и сферы применения.

Аддитивные технологии представляют собой одно из направлений цифрового производства. Позволяют изготавливать изделие послойно на основе компьютерной 3D-модели (CAD-модель). Аддитивные технологии – это совокупность технологий, которые создают 3D-объект, добавляя материал способом «слой-на-слой».

Общая схема аддитивного производства включает в себя последовательность этапов, представленных на схеме.



CAD-модель создается средствами САПР (систем автоматизированного проектирования).

STL – формат, который позволяет спроектированный на компьютере трехмерный объект преобразовать из 3d модели в программу, указывающую оборудованию траекторию и глубину резки материала. С файлами этого формата чаще всего сталкиваются операторы станков с ЧПУ, проектировщики, дизайнеры и пользователи ПК, осваивающие 3D-принтеры.

Виды 3D печати

SLA (стереолитография). Сегодня рынок 3D-печати растет по экспоненциальной зависимости. Уже есть более шести технологий 3D печати:

FDM (Fused Deposition Modeling) – принцип работы технологии заключается в послойном выращивании изделия из предварительно расплавленной пластиковой нити. Это самая распространенная технология 3D-печати в мире.

SLA (Laser Stereolithography) – cтереолитография (SLA или SL) технология аддитивного производства моделей, прототипов и готовых изделий из жидких фотополимерных смол. Отвердевание смолы происходит за счет облучения ультрафиолетовым лазером или другим источником энергии (засветка полимера слой за слоем).

SLS (Selective Laser Sintering, селективное лазерное спекание, выборочное лазерное спекание) – метод аддитивного производства, основан на последовательном спекании порошкового материала с помощью лазеров. Используется для создания функциональных прототипов и мелких партий готовых изделий.

SLM (Selective Laser Melting, селективное лазерное плавление) – распространенный метод трехмерной печати металлических изделий. В качестве материала используется металлический порошок очень мелкой фракции.

MJM (MultiJet Printing) – технология много струйного моделирования.

CJP (ColorJet Printing) – технология 3D-печати, в основе которой лежит послойное склеивание и окрашивание композитного порошка на основе гипса или пластика, метод цветной полимерной печати. В качестве сырья используются цветные порошки, которые слой за слоем наносятся на форму.

3D-сканер – устройство, предназначенное для быстрого анализа геометрии физического объекта и создания его точной компьютерной 3D-модели.

# Масштабы распространения киберугроз и основные виды киберугроз

Виды киберугроз

Кибербезопасность борется с тремя видами угроз:

1. Киберпреступления – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. Кибератака – действия, нацеленные на сбор информации, в основном политического характера.
3. Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Для получения контроля над компьютерными системами злоумышленники используют различные инструменты и приемы:

1. Вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы, они копируют себя сами. Они скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы.
2. Черви – в отличие от вирусов червям для распространения не требуется вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев.
3. Троянские программы – вредоносы, которые прячутся под маской легального программного обеспечения.
4. Шпионское программное обеспечение – программы, которые втайне следят за действиями пользователя и собирают информацию
5. Программы-вымогатели – шифруют, файлы и данные. Затем преступники требуют выкуп за восстановление и расшифровку, утверждая, что иначе пользователь потеряет данные.
6. Рекламное программное обеспечение – программы рекламного характера, с помощью которых может распространяться вредоносное программное обеспечение. Один из наиболее распространенных типов вредоносных программ. Adware – это программы, которые предназначены для показа рекламы на Вашем компьютере, перенаправления запросов поиска на рекламные вебсайты и сбора маркетинговой информации о Вас, чтобы реклама соответствовала Вашим интересам.
7. Боты – это программы, предназначенные для автоматического выполнения определенных операций. Хакеры могут также пытаться заразить несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть, которая затем будет использоваться для удаленного управления взломанными машинами.
8. Руткиты – позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT- специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества: проникнув на Ваш компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить Ваши данные или установить другие вредоносные программы. Руткиты умеют качественно маскировать свое присутствие в системе, чтобы оставаться незамеченными как можно дольше. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.
9. Баги – ошибки в фрагментах программного кода. Это не тип вредоносного программного обеспечения, а именно ошибки, допущенные программистом. Они могут иметь пагубные последствия для Вашего компьютера, такие как остановка, сбой или снижение производительности. В то же время баги в системе безопасности – это легкий способ для злоумышленников обойти защиту и заразить Ваше устройство. Обеспечение более эффективного контроля безопасности на стороне разработчика помогает устранить ошибки, но важно также регулярно проводить программные корректировки, направленные на устранение конкретных багов.
10. SQL-инъекция - вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL)
11. Спам – электронный эквивалент бумажной рекламы, которую обычно бросают в почтовый ящик. Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками, целью которых является распространить вредоносный код на компьютерах получателей. Для защиты от спама или совращения количества спама в электронный почтовый ящик целесообразно никогда не отвечать на спам.
12. Фишинг - – вид интернет-мошенничества, представляет собой атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя. Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.
13. Атаки Man-in-the-Middle — Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают.
14. DoS-атаки - Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.
15. Программы-вымогатели – троянские программы, предназначенные для вымогания денег у жертвы. Программы-вымогатели (ransomware) представляют собой тип вредоносного программного обеспечения, используемый киберпреступниками для получения выкупа. Существует два основных типа программ-вымогателей: шифровальщики и блокировщики.

Вредоносный код – это компьютерный код или веб-скрипт, преднамеренно разработанный для создания уязвимостей в системе, с помощью которых он выполняет несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем.

# Способы защиты от кибератак: советы по кибербезопасности

Самыми популярными мерами, применяемыми для защиты от киберугроз в мире и в России, являются антивирусная защита, клиентские межсетевые экраны, установка обновлений и резервное копирование данных. Прокомментируем более подробно способы защиты.

1. Обновление программного обеспечения и операционной системы. Использование нового программного обеспечения обеспечивает более надежные системы безопасности.
2. Использование антивирусных программ. Для максимальной безопасности регулярно следует обновлять программное обеспечение.
3. Использование надежных паролей. Не следует применять комбинации, которые легко подобрать или угадать.
4. Нельзя открывать почтовые вложения от неизвестных отправителей. Они могут быть заражены вредоносным программным обеспечением.
5. Нельзя переходить по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов. Это один из стандартных путей распространения вредоносного программного обеспечения. Адрес сайта, на котором Вы вводите платежные данные, должен начинаться с «https», а не с «http». Это значит, что сайт использует протокол защиты информации, который обеспечивает обмен данными исключительно между устройством и сервером.
6. Избегать незащищенных сетей Wi-Fi в общественных местах. В них Вы уязвимы для атак Man-in-the-Middle.

# Понятие о конфиденциальности и персональных данных

Конфиденциальность – это необходимость предотвращения разглашения, утечки какой-либо личной информации.

Персональные данные представляют собой информацию о конкретном человеке. 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.

Правила защиты персональных данных в сети Интернет:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми Вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.
4. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
5. Старайтесь периодически менять пароли.
6. Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и так далее).

Вирусы и антивирусные программы

Компьютерные вирусы – одна из самых старых форм вредоносного программного обеспечения. Вирусы самостоятельно копируют себя. Независимо от того, как вирус собирается проявиться его действия, отнимают ресурсы системы. Это замедляет работу компьютера и даже может совсем остановить ее, если вирус потребует слишком много ресурсов или если одновременно будут работать несколько вирусов. Чаще всего компьютерный вирус действует со злым умыслом – либо сам вирус написан как вредоносный, либо проблемы пользователю создают другие вредоносные программы, которые он устанавливает – черви и трояны.

Классификация вирусов:

1. Среда обитания:
   1. Сетевые - распространяются по компьютерным сетям
   2. Файловые – внедряются в файлы с расширением .com, .exe
   3. Загрузочные - внедряются в загрузочный сектор
   4. Файлово – загрузочные
2. Способ заражения
   1. Резидентные – оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение
   2. Нерезидентные – не заражают память компьютера и являются активными ограниченное время операционной системы к объектам заражения и внедряется в них
3. Степень воздействия
   1. Неопасные – не мешают работе компьютера, но уменьшают объем свободной памяти и памяти на дисках
   2. Опасные – могут привести к различным нарушениям в работе компьютера
   3. Очень опасные – приводят к потере программ, уничтожению данных, стиранию информации в системных областях диска
4. Особенности алгоритмов
   1. Паразитические – изменяют содержимое файлов и секторов диска и могут быть легко обнаружены и уничтожены
   2. Репликаторы (черви) - распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии
   3. Невидимки – трудно обнаружить и обезвредить, т. к. они перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска
   4. Мутанты – сложно обнаружить, содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют повторяющейся цепочки байтов
   5. Троянские – не способны к самораспространению, но очень опасны, т. к., маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Для защиты от вирусов следует убедиться, что на всех Ваших устройствах установлена последняя версия антивирусного ПО, которое может активно сканировать Вашу систему и противодействовать вирусам.

Антивирусная программа – это программа, предназначенная для обнаружения, удаления и защиты от компьютерных вирусов. Главной задачей антивируса является предотвращение заражения, еще одна его функция – удаление вредоносного ПО с зараженного компьютера. При использовании антивируса сканирование компьютера на наличие вредоносных программ играет ключевую роль в поддержании безопасности компьютера.

Виды антивирусов:

1. Детекторы - осуществляют поиск характерной для конкретного вируса последовательности байтов в оперативной па-мяти и в файлах и при обнаружении выдают соответствующее сообщение.
2. Ревизоры – запоминают исходное состояние программ, каталогов и системных областей диска до заражения вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние и исходным.
3. Вакцины – резидентные программы, предотвращающие заражение файлов.
4. Доктора - находят зараженные вирусами файлы и «лечат» их, т. е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние.
5. Фильтры - предназначены для обнаружения подозрительных действий при работе компьютера.

Защита компьютера от вирусов

Работа в Интернете делает компьютер уязвимым для вредоносных программ-вирусов. Чтобы предотвратить заражение, придерживайтесь следующих правил:

1. Регулярно обновляйте браузер, операционную систему и антивирусную базу. Браузер Chrome автоматически обновляется до последней версии при каждом запуске, обеспечивая надёжную защиту без усилий со стороны пользователя.
2. Проверяйте адреса сайтов, не загружайте неизвестные файлы с расширением .exe, .dll, .bat и не переходите по ссылкам из всплывающих окон.
3. Если ваши действия привели к блокировке экрана подозрительным сообщением, закройте браузер в диспетчере задач или мониторе активности своей операционной системы.
4. Загружайте ПО только с официальных сайтов-разработчиков.
5. При неадекватной работе ПО (устройство медленно работает, появляются всплывающие окна, выполняются непонятные платежи) сразу удалите его с помощью последней версии антивирусной программы.
6. Выбирайте зарекомендовавшие себя антивирусные программы и устанавливайте только лицензионные версии.
7. Установите следующие настройки антивирусной программ
   1. включите проактивный и поведенческий анализ – эти режимы позволяют отловить вредоносные программы, которых ещё нет в антивирусной базе;
   2. настройте проверку почтовых сообщений и их вложений;
   3. проводите полное сканирование компьютера и подключаемых устройств не реже 1 раза в неделю.
   4. Не устанавливайте на компьютер сразу несколько средств защиты. Программы распознают друг друга как вредоносное ПО и начинают конкурировать между собой или вообще перестают работать.