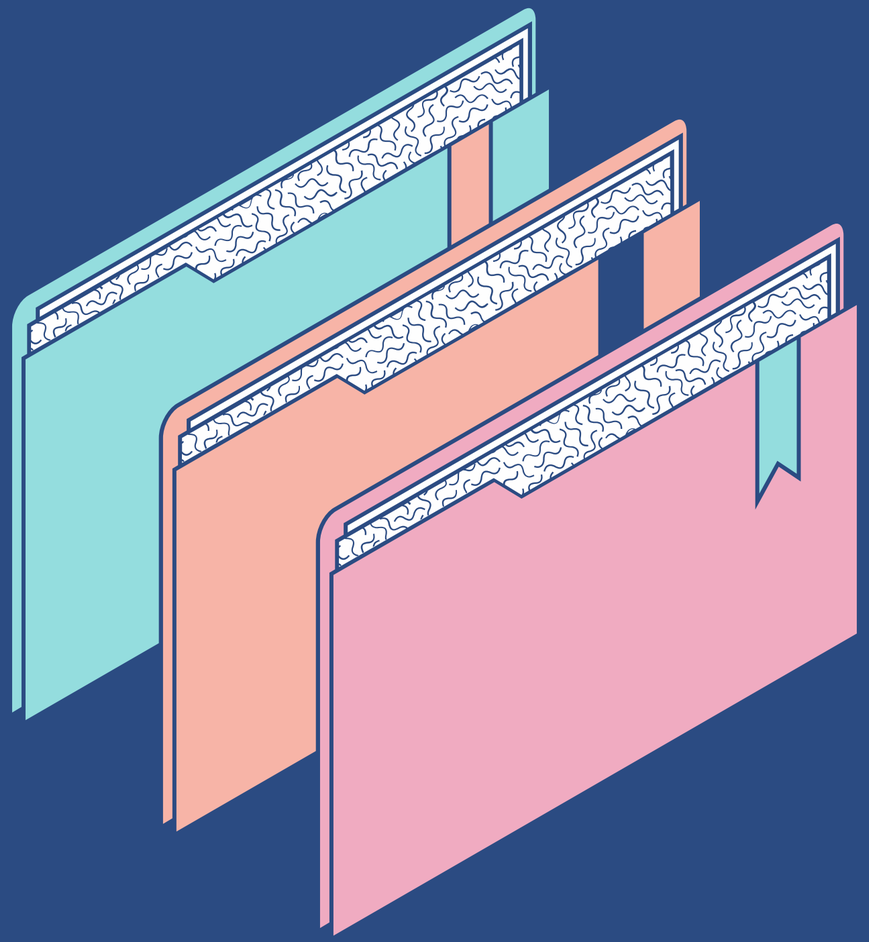
Основы кибербезопасности в НКО

БАХТИН ВАДИМ ВЯЧЕСЛАВОВИЧ

СТАРШИЙ ПРЕПОДАВАТЕЛЬ КАФЕДРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СИСТЕМ СВЯЗИ (ИБСС) ПГНИУ, НАУЧНЫЙ СОТРУДНИК КАФЕДРЫ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ (АТ) ПНИПУ



Повестка дня

КЛЮЧЕВЫЕ АСПЕКТЫ В ПРЕЗЕНТАЦИИ

- Принципы обеспечения кибер- и информационной безопасности в НКО
- Как правильно обращаться с цифровыми данными НКО
- "Безопасные" сервисы и платформы для хранения, использования и передачи цифровых данных
- Принципы защиты веб-сайтов и информационных каналов НКО от взломов и хакерских атак

Принципы (правила) обеспечения кибер- и информационной безопасности в НКО

Развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности.

Информационная безопасность - совокупность средств, методов и процедур, обеспечивающих защиту информационных активов и гарантирующих сохранение технической инфраструктуры информационных систем и сведений, которые в таких системах хранятся и обрабатываются.

Угрозы безопасности информации - события или действия, которые могут привести к искажению, несанкционированному использованию или к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Информационная безопасность включает

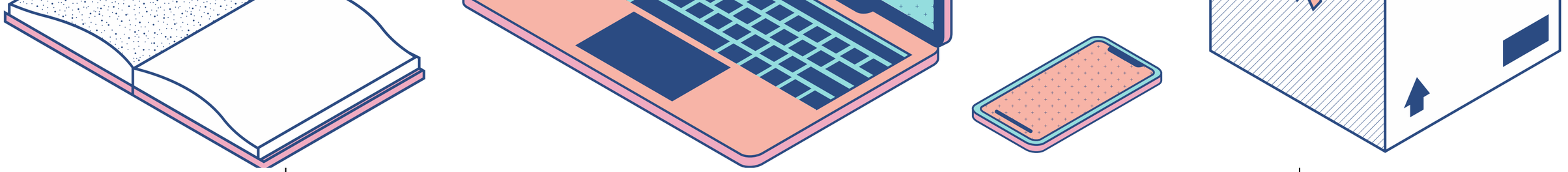
1. *Состояние защищенности информационного пространства*, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;

2. *Состояние инфраструктуры*, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;

3. *Состояние информации*, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;

4. *Экономическую составляющую* (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами,

5. *Финансовую составляющую* (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов)



Информационная безопасность

- Политика безопасности
  - Объект информационной безопасности
  - Угрозы объекту информационной безопасности
  - Обеспечение информационной безопасности
    - Методы обеспечения информационной безопасности
    - Деятельность по обеспечению информационной безопасности (по недопущению вреда объекту информационной
    - Средства осуществления деятельности по обеспечению информационной безопасности
    - Субъекты обеспечения информационной безопасности

Понятие информационной безопасности в узком смысле этого слова подразумевает

- Надежность работы компьютера
- Сохранность ценных данных
- Защиту информации от внесения в нее изменений
- Сохранение тайны переписки в электронной связи

Защита информации

ЗАКОННОСТЬ И ОБОСНОВАННОСТЬ ЗАЩИТЫ

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

СИСТЕМНОСТЬ

Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:при всех видах информационной деятельности и информационного проявления; во всех структурных элементах; при всех режимах функционирования;на всех этапах жизненного цикла; с учетом взаимодействия объекта защиты с внешней средой.

КОМПЛЕКСНОСТЬ

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

ОТКРЫТОСТЬ АЛГОРИТМОВ И МЕХАНИЗМОВ ЗАЩИТЫ

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты.

Защита информации

НЕПРЕРЫВНОСТЬ ЗАЩИТЫ

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

РАЗУМНАЯ ДОСТАТОЧНОСТЬ

Создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточных времени и средствах можно преодолеть любую защиту. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

ГИБКОСТЬ

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

ПРОСТОТА ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

Концепция комплексной защиты

Эффективное обеспечение защиты информации возможно только на основе комплексного использования всех известных методов и подходов к решению данной проблемы.

Разработка и доведение до уровня регулярного использования всех необходимых механизмов гарантированного обеспечения требуемого уровня защищенности информации

Существование механизмов практической реализации требуемого уровня защищенности

Наличие средств рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники

Разработка способов оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации.

Не существует таких методов и средств защиты, которые позволили бы абсолютно надежно и полно защитить информацию от несанкционированных действий. Вместо этого в информационной безопасности разрабатываются и применяются меры, существенно затрудняющие деятельность злоумышленника.

Как правильно хранить, использовать, переносить данные НКО

У каждой компании по закону должен быть свой архив для хранения документов. В случае некоммерческих организаций порядок обращения с документами строго регламентирован.

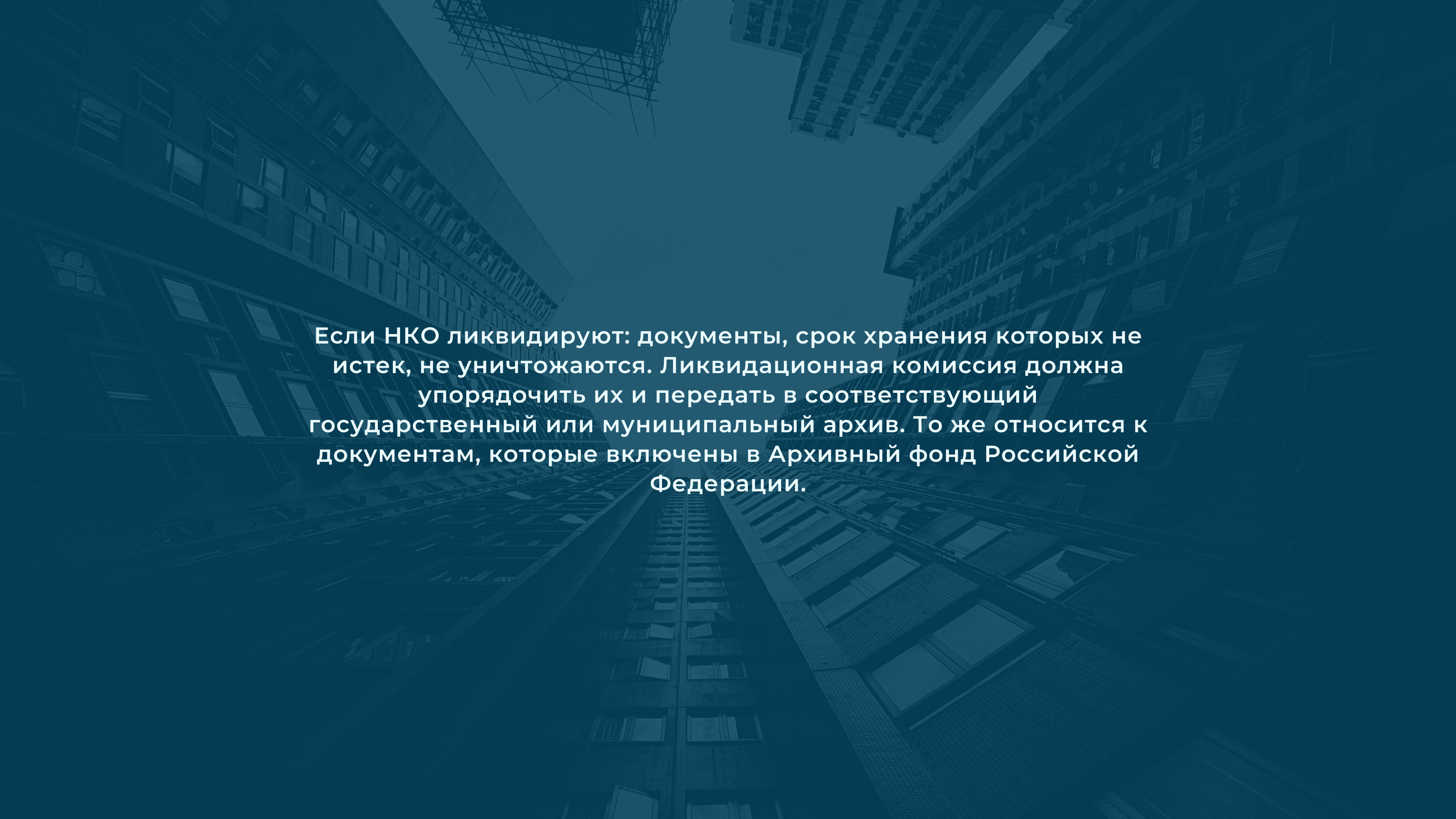
Первичные учетные документы, регистры бухгалтерского учета, финансовую отчетность и аудиторские заключения НКО должны хранить не менее пяти лет после отчетного периода.

Перечень «вечных» документов

К «вечным» документам относятся:

- протокол учредительного собрания
- устав
- положения о филиалах или представительствах
- штатное расписание
- годовая финансовая отчетность (бухгалтерские балансы, отчеты о финансовых результатах, отчеты о целевом использовании средств, приложения к ним)
- положения об обработке персональных данных, документы о рассмотрении и утверждении финансовой отчетности, протоколы контрольных, ревизионных органов организации
- документы о реорганизации НКО и документы о ликвидации.

Срок действия оперативных планов, журналов учета работников, совмещающих должности, проекты уставов, положений и документов по их разработке организация определяет сама.



Если НКО ликвидируют: документы, срок хранения которых не истек, не уничтожаются. Ликвидационная комиссия должна упорядочить их и передать в соответствующий государственный или муниципальный архив. То же относится к документам, которые включены в Архивный фонд Российской Федерации.

БЕЗОПАСНОСТЬ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ МОЖЕТ БЫТЬ ОБЕСПЕЧЕНА ЛИШЬ В СЛУЧАЕ СИСТЕМНОГО ПОДХОДА.

УПРАВЛЕНИЕ ПАРОЛЯМИ И СОЗДАНИЕ СЛОЖНЫХ ПАРОЛЕЙ

Пароль — базовый способ защиты ваших данных. К его выбору стоит подходить аккуратно. Примитивные наборы подбираются достаточно быстро с помощью специального софта.

ШИФРОВАНИЕ ВАЖНЫХ ДОКУМЕНТОВ НА ЛОКАЛЬНОМ КОМПЬЮТЕРЕ

Существуют разные мнения о необходимости шифрования информации. Но шифрование может дать дополнительную защиту от хакеров, перехвата данных и других атак злоумышленников.

УСТАНОВКА ДОПОЛНИТЕЛЬНОЙ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ВХОДА В АККАУНТЫ

Для этого понадобится включить — там, где это возможно — двухфакторную аутентификацию. Это дополнительная защита аккаунтов в соцсетях, мессенджерах, электронной почте, Apple, Google и т.п.

PGP-ШИФРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Необходимо обезопасить конфиденциальную переписку и обмен файлами по электронной почте. Благодаря этому можно шифровать отправляемую почту и, в обратном порядке, – расшифровывать входящую с помощью пары PGP-ключей.

БЕЗОПАСНОСТЬ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ МОЖЕТ БЫТЬ ОБЕСПЕЧЕНА ЛИШЬ В СЛУЧАЕ СИСТЕМНОГО ПОДХОДА.

ИСПОЛЬЗОВАНИЕ АНТИВИРУСА

Существуют три основных типа угроз – вредоносные программы, фишинг и мобильные угрозы, от которых вас могут защитить антивирусы. Антивирусы защищают от вредоносных программ. Вирусы – это не единственные вредоносные программы.

ИСПОЛЬЗОВАНИЕ УДАЛЕННЫХ (ОБЛАЧНЫХ) ХРАНИЛИЩ ДАННЫХ

В случае утраты какого-либо из устройств вы не потеряете информацию.

ВВОД ВАЖНОЙ ИНФОРМАЦИИ ТОЛЬКО НА САЙТАХ С ЗАЩИЩЕННЫМ СОЕДИНЕНИЕМ

Любую информацию — от ввода логина и пароля до номера банковской карты и вашей фамилии — стоит отправлять только с ресурсов, где включён HTTPS.

МИНИМИЗИРУЙТЕ ВОЗМОЖНОСТЬ ПОДСМОТРЕТЬ ЗА ВАМИ И ПОДСЛУШАТЬ ВАС

Злоумышленники или спецслужбы, используя специальное программное обеспечение и уязвимости вашего софта, могут подключиться к микрофону и камере вашего компьютера, телефона или планшета.

Обработка персональных данных

Если в НКО собирают, записывают, систематизируют, накапливают, хранят, уточняют (обновляют), используют, передают (распространяют, предоставляют), обезличивают, удаляют и уничтожают персональные данные, то все это, как следует из закона, является обработкой персональных данных.

Обрабатывать персональные данные не запрещено, но делать это нужно при соблюдении законодательства.

ЧТО НУЖНО СДЕЛАТЬ НКО ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Перечень мер, направленных на защиту персональных данных, организация вправе определять самостоятельно. Здесь будут перечислены лишь минимум таких мер

Разработать и принять Положение об обработке персональных данных.

Назначить приказом руководителя организации ответственного сотрудника, обеспечивающего исполнение организацией законодательства о персональных данных.

Получить от каждого субъекта согласие на обработку персональных данных.

Уведомить субъект персональных данных о прекращении обработки и об уничтожении его персональных данных.

После того как вы закончите, скачайте вашу презентацию Canva в формате MP4 или получите ссылку, чтобы поделиться ею со слушателями.

Осуществить технические меры защиты персональных данных (например, хранить документы с персональными данными в запираемых на замок шкафах.

ЧТО НУЖНО СДЕЛАТЬ НКО ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Ознакомить сотрудников с действующим законодательством в области защиты персональных данных и локальными актами организации об этом

Провести профилактическую работу с сотрудниками организации по предупреждению разглашения ими персональных данных

Разместить информацию о том, как организована работа с персональными данными в организации (положение об обработке персональных данных или политика конфиденциальности в организации) в доступном для людей месте в офисном помещении, опубликовать ее в интернете, если у организации есть сайт, а также на всех онлайн ресурсах организации, которые собирают персональные данные пользователей.

"Безопасные" сервисы и платформы для хранения, использования и передачи цифровых данных

Облачные сервисы

ДЛЯ ХРАНЕНИЯ, ИСПОЛЬЗОВАНИЯ И ПЕРЕДАЧИ ЦИФРОВЫХ ДАННЫХ ПРИБЕГАЮТ К ИСПОЛЬЗОВАНИЮ СПЕЦИАЛЬНЫХ ОБЛАЧНЫХ СЕРВИСОВ. ТРИ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ МОДЕЛИ ОБЛАЧНЫХ УСЛУГ:

Infrastructure as a Service (IaaS)

инфраструктура как услуга

Platform as a Service (PaaS)

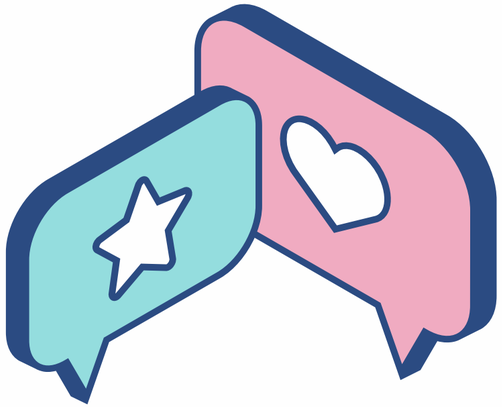
платформа как услуга

Software as a Service (SaaS)

программное обеспечение как услуга

Что такое IaaS?

Инфраструктура как услуга (IaaS) — это предоставление вычислительных ресурсов через облако. В качестве готового решения клиент может выбрать: хранилище данных, виртуальный сервер, операционную систему и количество ресурсов. IaaS часто используют те, кто хочет избавиться от необходимости поддерживать собственные локальные центры обработки данных.

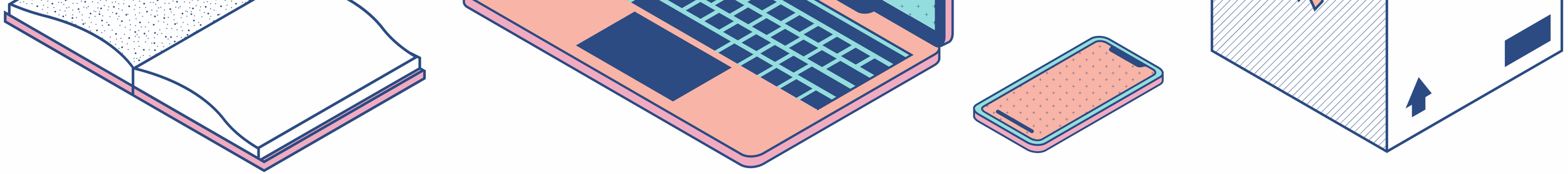


Infrastructure as a Service

- Покупка собственного серверного оборудования не требуется, так как клиент арендует его у провайдера IaaS и получает в виртуальном виде через облачные серверы.

- Они предоставляются организации через панель управления, например, VMware — цифровая платформа на базе облачных технологий позволяет работать с любыми программами в различных облаках и на большом количестве устройств. С помощью этого клиенты полностью контролируют всю инфраструктуру и могут настроить ее под нужды организации.

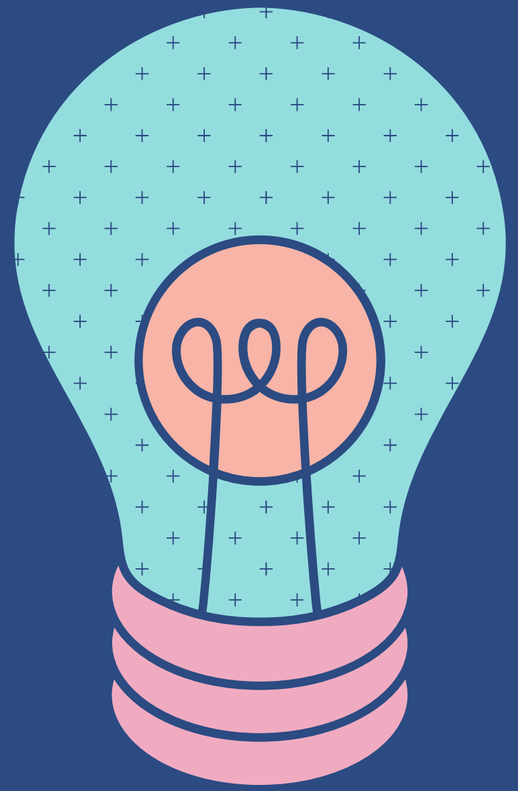
- Пользователи IaaS самостоятельно управляют приложениями, операционными системами и специализированным ПО, а провайдер поддерживает работу серверов, СХД и другого физического оборудования.



Преимущества IaaS

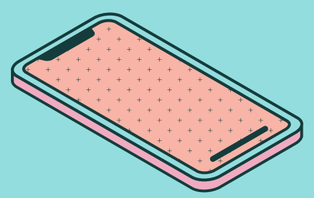
- IaaS — это наиболее гибкая модель облачных услуг с простым процессом развертывания оборудования.
- IaaS позволяет предприятиям наращивать вычислительные ресурсы по мере необходимости, вместо того, чтобы покупать дорогостоящее оборудование для собственной инфраструктуры. Например, цена сервера Cisco UCS в среднем начинается от 1 млн рублей.
- Стоимость IaaS варьируется и в основном зависит от потребностей клиента в CPU и RAM. IaaS — это также экономичная модель, в том числе из-за высокой масштабируемости и автоматизации облачных услуг.

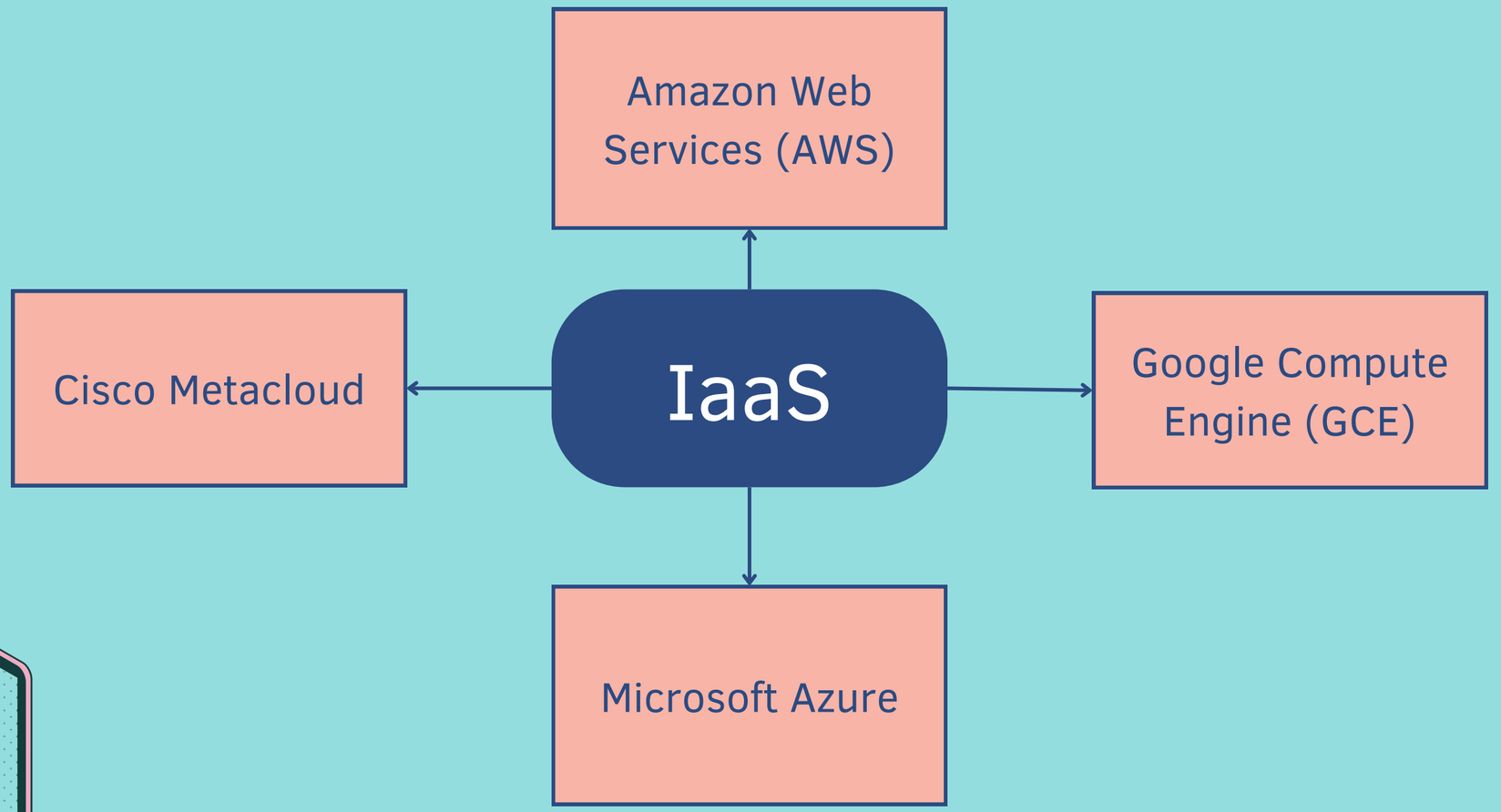
Услуги IaaS актуальны как для стартапов и небольших компаний, так и крупного бизнеса. Облачные сервисы — альтернатива покупке оборудования и созданию локальной инфраструктуры. С ростом потребностей, компаниям приходится внедрять новые сервисы и приложения, в чем помогает гибкость облачных услуг. Простыми словами: переход на IaaS экономит время и деньги.



КОМУ ПОДХОДИТ IAAS?

Наиболее известные примеры IaaS





Что такое PaaS?

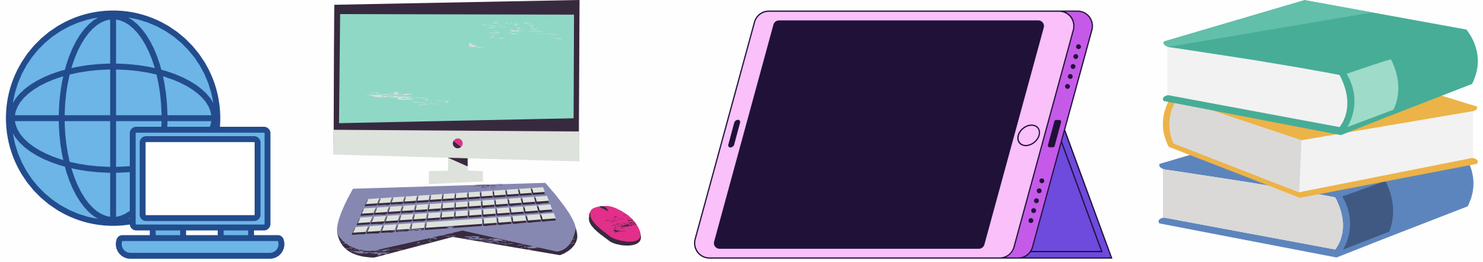
Платформа как услуга (PaaS) предоставляет настраиваемую среду для разработчиков. Клиенты получают доступ к платформе или набору инструментов для создания приложений через интернет. С помощью услуг PaaS разработчики могут создавать всё, от простых мобильных приложений до сложного программного обеспечения для бизнеса.

Преимущества PaaS

- Подобно другим облачным сервисам, PaaS позволяет клиентам пользоваться современными мощными инструментами разработки, поддержку которых берет на себя провайдер. Платформа как услуга хороша тем, что сразу же готова к работе.

- С помощью PaaS повышается скорость разработки, тестирования и доставки приложений. На готовой платформе команде разработчиков будет проще и экономичнее реализовывать проекты любого размера и сложности — затраты на развертывание платформы и промежуточного ПО берёт на себя провайдер.

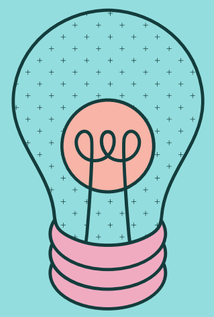
- Облачные технологии позволяют увеличивать/уменьшать ресурсы при необходимости. Несколько пользователей могут получить доступ к проекту через одну и ту же платформу, которая в свою очередь может работать с разными веб-службами и базами данных.

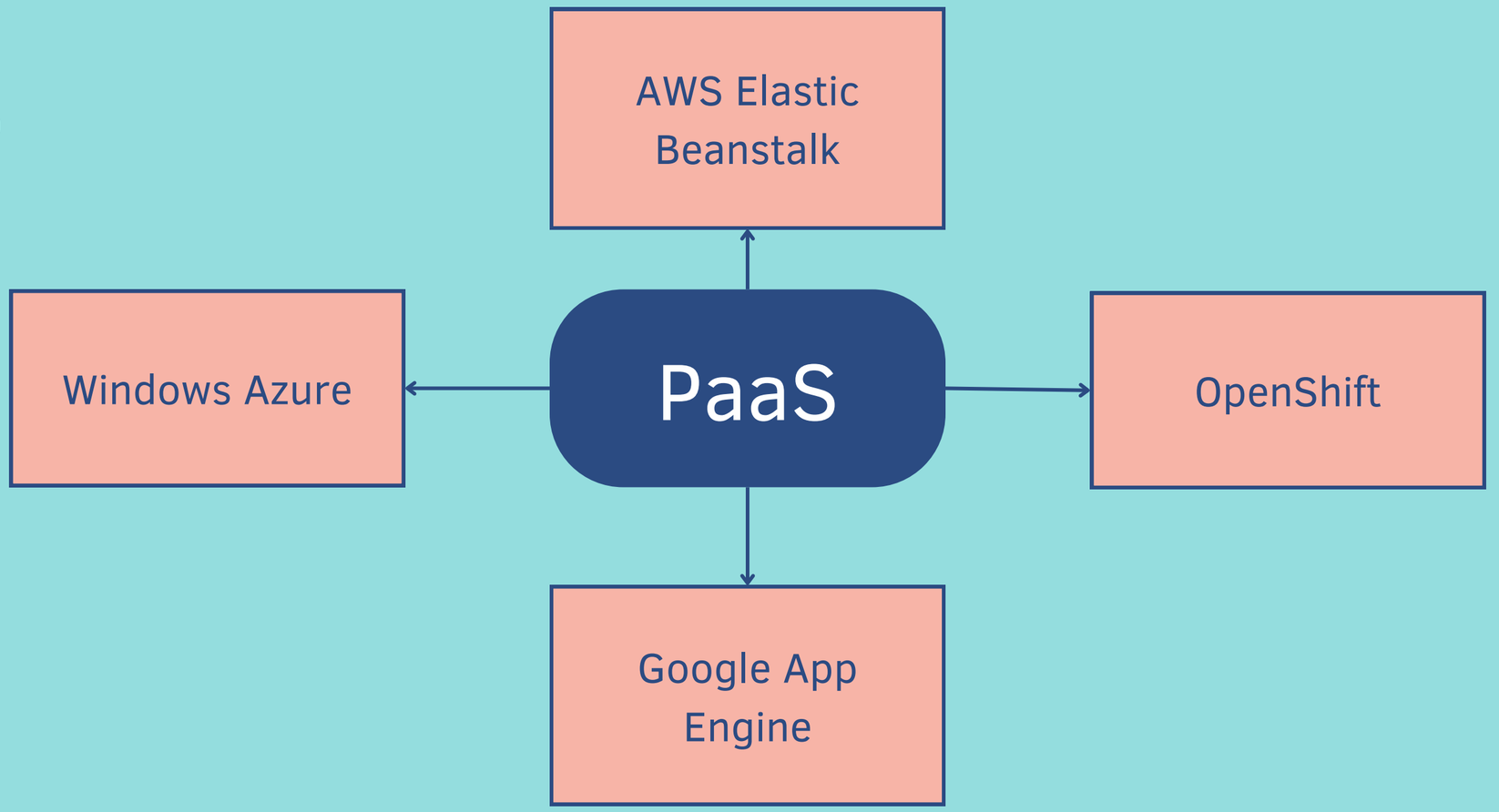


Кому подходит PaaS?

- Решения PaaS помогают компаниям разного размера оптимизировать процесс разработки. Например, PaaS может упростить работу большой команды разработчиков, которые занимаются одним и тем же проектом.
- Этот вариант может оказаться предпочтительным для компаний с существующей ИТ-инфраструктурой. Клиентам понадобятся собственные ИТ-специалисты для использования и настройки программного обеспечения PaaS-платформы, но взамен организация получит больший контроль над процессом разработки и последующую гибкость поставки готового приложения клиентам.

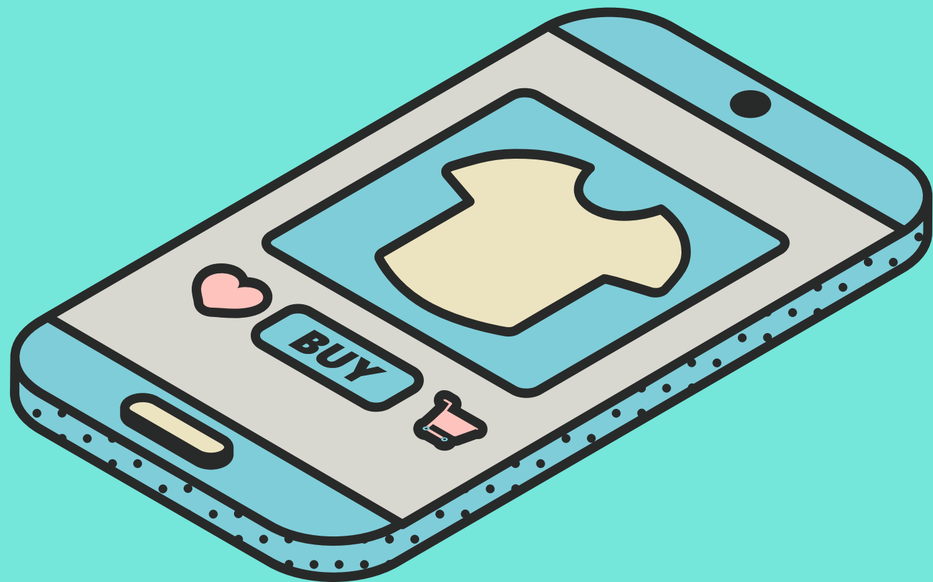
Наиболее известные примеры PaaS





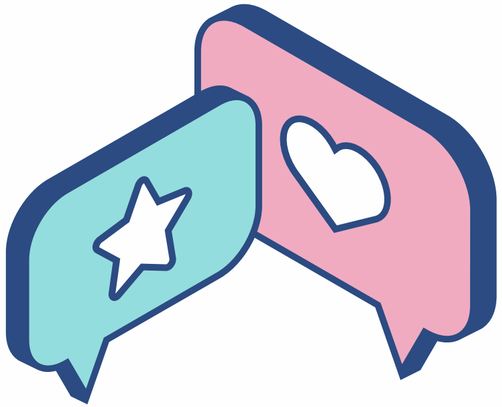
Что такое SaaS?

Программное обеспечение как услуга (SaaS) — это предоставление клиентам уже настроенных программ для различных бизнес-задач через интернет. В качестве SaaS-решений могут предоставляться CRM, ERP, ITSM-системы, таск-трекеры и другое ПО.



Преимущества SaaS

Удаленная, настройка и обслуживание ПО провайдером предоставляет компании-заказчику больше времени для решения других важных вопросов и задач. SaaS-решения управляются централизованно и размещаются на удаленном сервере. Производитель, а не пользователь, несет ответственность за настройку необходимого оборудования и программного обеспечения.
Чаще всего для работы SaaS не требуется загрузка и установка ПО на устройство, — большинство программ запускаются в браузере.

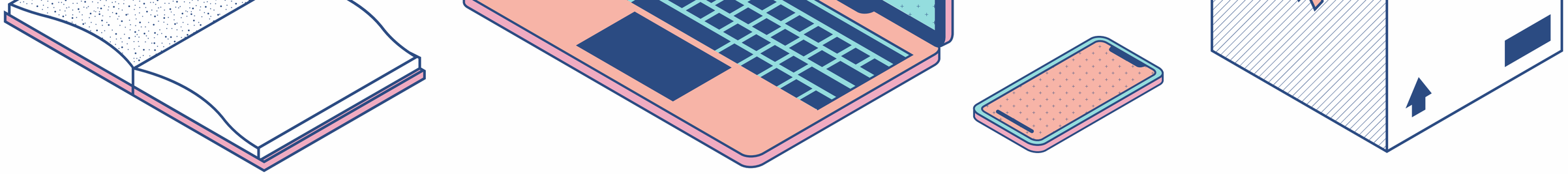


Кому подходит SaaS?

- Использование услуг SaaS выгодно для компаний, у которых нет возможности покупать on-premise-решения. Крупные компании могут использовать эту модель для краткосрочных проектов, требующих быстрых, простых и доступных решений.

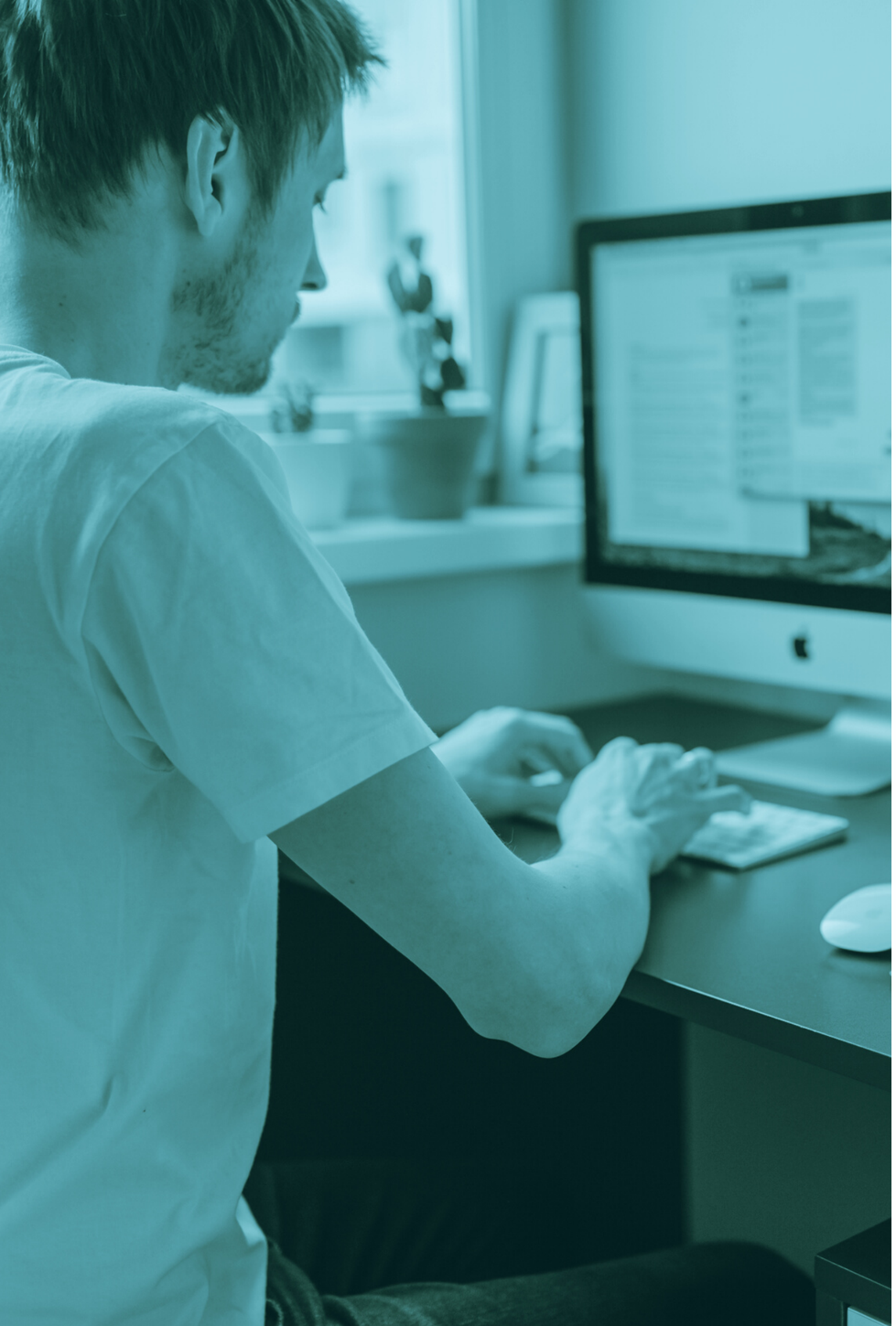
- Также услуги этой модели подходят клиентам, которым нужно приложение, доступное через интернет, в том числе с мобильного устройства.

- SaaS предоставляет решения для разных задач. Например, CRM-системы помогают автоматизировать взаимодействие компании с заказчиками, ERP-системы — оптимизировать управление ресурсами предприятия, ITSM-системы — упростить предоставление и поддержку ИТ-услуг.



Наиболее известные примеры SaaS

- Salesforce
- Service Now
- Google Workspace
- SAP
- Cisco WebEx
- 1С в облаке
- Worksection
- SimpleOne



Какую модель выбрать?

Каждая облачная модель предлагает определенные функции и возможности. Когда у бизнеса есть набор конкретных задач и понимание преимуществ разных типов облачных сервисов, проще выбрать подходящий.

Закрепление материала

ПЛЮСЫ КАЖДОЙ МОДЕЛИ В СРАВНЕНИИ

Infrastructure as a Service (IaaS)

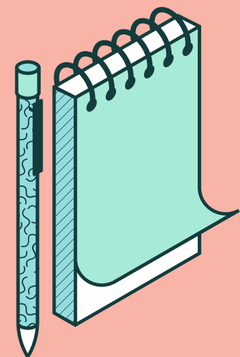
Решения IaaS дают практически полный контроль над готовой инфраструктурой, что позволяет организации создать стек технологий, полностью адаптированный к потребностям бизнеса.

Platform as a Service (PaaS)

Предприятия, которые уже обладают некоторыми ресурсами и ИТ-отделом, могут выбрать сервисы PaaS: готовая платформа поможет компаниям разрабатывать индивидуальные решения, которые легче интегрировать с существующими рабочими процессами.

Software as a Service (SaaS)

Услуги SaaS позволяют предприятиям экономить деньги: клиентам не нужно самостоятельно заниматься разработкой и поддержкой программного обеспечения.



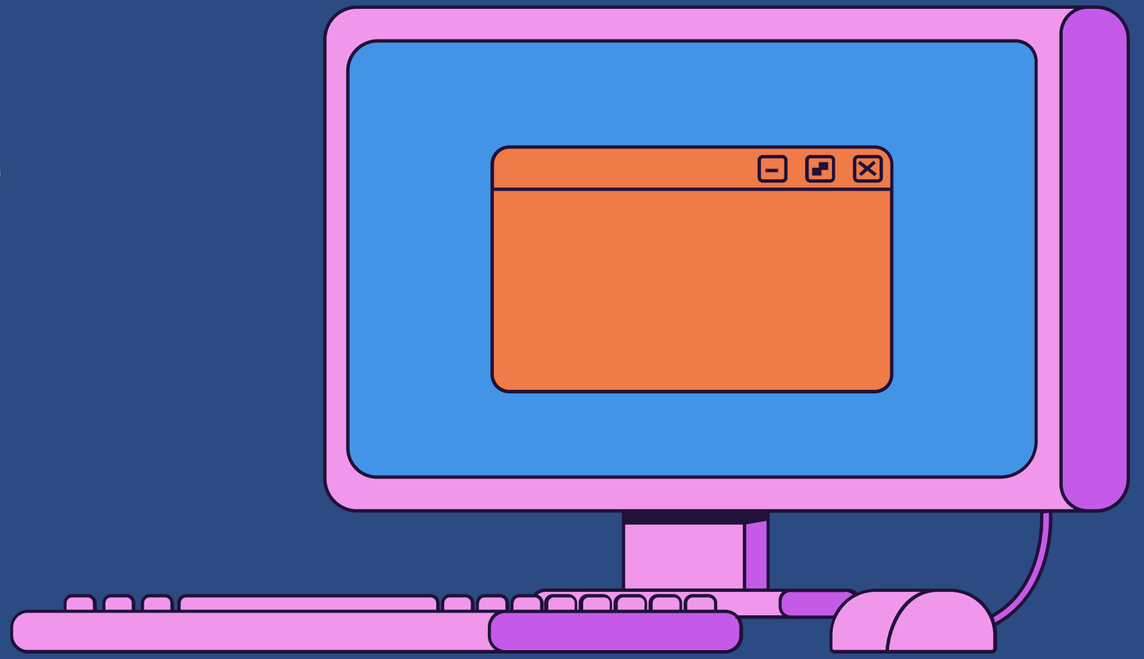
Применение

ЕСЛИ ВЫ РЕШИЛИ УПРАВЛЯТЬ СОБСТВЕННОЙ ИНФРАСТРУКТУРОЙ, НЕОБХОДИМО ВЫПОЛНИТЬ УКАЗАННЫЕ НИЖЕ ДЕЙСТВИЯ.

1. Приобретите физический сервер.
2. Установите на него все необходимое программное обеспечение и операционные системы.
3. Напишите код приложения электронной почты и установите его на сервер.
4. Постоянно выполняйте обслуживание аппаратного и программного обеспечения.
5. Наслаждайте оптимизацией рабочего процесса.

SaaS, PaaS и IaaS предоставляют разные уровни услуг. Однако в любом случае, облачные решения снимают работу с клиентов и помогают экономить время, усилия сотрудников и деньги. Облако — это будущее технологий для развития бизнеса.

ИТОГ



ПРИНЦИПЫ ЗАЩИТЫ ВЕБ-САЙТОВ И ИНФОРМАЦИОННЫХ КАНАЛОВ НКО ОТ ВЗЛОМОВ И ХАКЕРСКИХ АТАК.

ГРУПП В СОЦИАЛЬНЫХ СЕТЯХ, ЭЛЕКТРОННОЙ ПОЧТЫ

ВЕБ-ПРИЛОЖЕНИЯ

— ЭТО НЕОТЪЕМЛЕМАЯ ЧАСТЬ РАБОЧЕГО ПРОЦЕССА БОЛЬШИНСТВА ОРГАНИЗАЦИЙ — АБС СИСТЕМЫ БАНКОВ, CRM, 1С И ДРУГИЕ ПРОГРАММЫ, КОТОРЫМИ ЕЖЕДНЕВНО ПОЛЬЗУЮТСЯ СОТРУДНИКИ. ОНИ АККУМУЛИРУЮТ В СЕБЕ ОГРОМНОЕ КОЛИЧЕСТВО ДАННЫХ, ОБЛАДАЮЩИХ ЦЕННОСТЬЮ. ПОЭТОМУ СПОСОБСТВОВАТЬ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ — ОДНА ИЗ КЛЮЧЕВЫХ ЗАДАЧ ДЛЯ МИНИМИЗАЦИИ ФИНАНСОВЫХ И РЕПУТАЦИОННЫХ РИСКОВ.

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

– ЭТО ЗАЩИТНЫЕ МЕРЫ, ПРИ КОТОРЫХ ЗЛОУМЫШЛЕННИК НЕ СМОЖЕТ ПОЛУЧИТЬ ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ КАК ИЗВНЕ ПРИ ПОПЫТКЕ ВЗЛОМА, ТАК И ВНУТРИ КОМПАНИИ ЧЕРЕЗ НЕЛЕГИТИМНЫЙ ДОСТУП.

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

НАИБОЛЕЕ РАСПРОСТРАНЕННАЯ УГРОЗА БЕЗОПАСНОСТИ **WEB-**ПРИЛОЖЕНИЙ

– ЭТО ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ, А ПРИ ПОПУЛЯРИЗАЦИИ ПРИЛОЖЕНИЯ В ИНТЕРНЕТЕ – НЕ ИЗБЕЖАТЬ И DDOS-АТАК. ДЛЯ ВЗЛОМА И ВЫВОДА ПРИЛОЖЕНИЯ ИЗ СТРОЯ МОГУТ ИСПОЛЬЗОВАТЬСЯ РАЗЛИЧНЫЕ ИНСТРУМЕНТЫ КАК ЛЮБИТЕЛЬСКИЕ, ТАК И ПРОФЕССИОНАЛЬНЫЕ КИБЕРАТАКИ И ИСПОЛЬЗОВАНИЕ АВТОМАТИЧЕСКИХ СИСТЕМ СКАНИРОВАНИЯ ДЛЯ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ.

АТАКИ МОЖНО УСЛОВНО ПОДЕЛИТЬ НА ДВЕ КАТЕГОРИИ УГРОЗ ИБ:

1. *Атаки, в которых цель состоит в том, чтобы отключить целевой компьютер или отключить его в автономном режиме*

2. *Атаки, цель которых состоит в том, чтобы получить доступ к данным целевого компьютера и, возможно, получить от них привилегии администратора*

ПРИНЦИПЫ ВЕБ-БЕЗОПАСНОСТИ

КОНФИДЕНЦИАЛЬНОСТЬ

Конфиденциальность означает, что неавторизованная сторона/частное лицо не может получить доступ к конфиденциальным данным организации. Если кому-то удается получить доступ посредством непреднамеренного поведения, то такое нарушение конфиденциальности называется нарушением.

ЦЕЛОСТНОСТЬ

Целостность заключается в том, чтобы гарантировать, что информация не будет изменена, или гарантировать, что подлинность данных будет сохранена.
Например, если у вас есть веб-сайт НКО, и кто-то пытается изменить документацию или что то подобное(), а вы не можете изменить данные, это означает нарушение целостности информации.

ДОСТУПНОСТЬ

Это означает, что доступ к информации осуществляется авторизованным пользователем, когда это необходимо. Информация ценна только в том случае, если она может быть доступна в нужное время. Отказ в обслуживании — очень распространенная атака в наши дни. Основная цель DOS — запретить пользователям доступ к21 ресурсам или информации, к которым у них есть доступ. Такие простои обходятся очень дорого. Вы можете обеспечить доступность, сохраняя резервную копию, которая может сохранить информацию в таких ситуациях, как DDOS атака, повреждение системы или оборудования.

ПРИНЦИПЫ ВЕБ-БЕЗОПАСНОСТИ

АУТЕНТИФИКАЦИЯ

Процесс, который определяет, является ли кто-либо на самом деле тем, за кого он себя выдает. Если учетные данные совпадают, пользователю предоставляется доступ, а если учетные данные различаются, аутентификация завершается сбоем, и в доступе отказано.

Здесь учетные данные сравниваются с файлами в базе данных авторизованных пользователей на сервере. Когда процесс завершен, пользователь имеет право просматривать или получать доступ и иметь права доступа к информации.

АВТОРИЗАЦИЯ

Аутентификация предшествует авторизации.

Получив доступ к системе, пользователь может попытаться выполнить команду. Авторизация определяет, имеет ли пользователь полномочия для выполнения команд.

ПОДОТЧЕТНОСТЬ

Это гарантирует, что действия объекта могут быть отслежены, и все его операции могут быть идентифицированы.

С другой стороны, подотчетность заключается в том, что сотрудник несет ответственность за выполнение задачи и должен будет объяснить, почему он выполняет не правомерные действия которые могут привести к нарушению информационной безопасности.

ПРИНЦИПЫ ВЕБ-БЕЗОПАСНОСТИ

НЕОТКАЗУЕМОСТЬ

состояние информации, при котором субъект не может отказаться от того действия, которое имело место быть. Человек не может отказаться от действия или информации, которую он отправил (например, средство обеспечения неотказуемости: подпись документа, ЭЦП).

АУТЕНТИЧНОСТЬ

свойство, гарантирующее, что субъект или ресурс идентичны заявленным. То есть, нарушение аутентичности, например, заражение вирусом – система не идентична заявленным, появились новые свойства. Подмена сервера, перенаправление на свой сервер и вытягивание данных. По сути – когда нет подмены, принципы работы остаются теми же. Действительно ли информация не изменялась. Может быть нарушена на этапе эксплуатации.

РЕКОМЕНДАЦИИ, КОТОРЫЕ ПОМОГУТ ЗАЩИТИТЬ ВЕБ-САЙТ ОТ БУДУЩИХ ХАКЕРСКИХ АТАК:

1. ОБЕСПЕЧИТЬ ЗАЩИТУ ОТ DDOS(АТАКА КОТОРАЯ ПРИВОДИТ К ОТКАЗУ СИСТЕМЫ)-АТАК
2. ПОДКЛЮЧИТЬ SSL-СЕРТИФИКАТ
3. ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ХОСТИНГ
4. ИСПОЛЬЗОВАТЬ БЕЗОПАСНЫЕ ПЛАГИНЫ, БИБЛИОТЕКИ, ФРЕЙМВОРКИ, CMS ПРИ РАЗРАБОТКЕ

РЕКОМЕНДАЦИИ, КОТОРЫЕ ПОМОГУТ ЗАЩИТИТЬ ВЕБ-САЙТ ОТ БУДУЩИХ ХАКЕРСКИХ АТАК:

5 ПРИМЕНЯТЬ СУЩЕСТВУЮЩИЕ ТЕХНИКИ ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ И XSS-АТАК

6 ОБЕСПЕЧИТЬ ВЕДЕНИЕ ЖУРНАЛА ВЕБ-САЙТА И МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

7 ЗАБОТА О БЕЗОПАСНОСТИ ПОСЕТИТЕЛЕЙ

8 ИСПОЛЬЗОВАТЬ БЕЗОПАСНЫЕ ПЛАГИНЫ, БИБЛИОТЕКИ, ФРЕЙМВОРКИ, CMS ПРИ РАЗРАБОТКЕ

РЕКОМЕНДАЦИИ, КОТОРЫЕ ПОМОГУТ ЗАЩИТИТЬ ВЕБ-САЙТ ОТ БУДУЩИХ ХАКЕРСКИХ АТАК:

9 ИСПОЛЬЗОВАТЬ НАДЕЖНЫЕ И СЛОЖНЫЕ ПАРОЛИ, А ТАКЖЕ ЗАЩИТУ ОТ ПЕРЕБОРА ПАРОЛЕЙ

10 ЕСЛИ ЕСТЬ АДМИНИСТРАТИВНАЯ ПАНЕЛЬ, С ПОМОЩЬЮ КОТОРЫЙ ПРОИСХОДИТ УПРАВЛЕНИЕ СОДЕРЖИМЫМ ВЕБ-САЙТА, НЕОБХОДИМО ИЗМЕНИТЬ СТАНДАРТНЫЙ АДРЕС ВХОДА И ОБЕСПЕЧИТЬ КОНТРОЛЬ ДОСТУПА

НАДЕЖНЫЙ ХОСТИНГ И SSL

SSL - СЕРТИФИКАТ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ МЕРОЙ, ПРОТОКОЛ БЕЗОПАСНОСТИ, СОЗДАЮЩИЙ ЗАШИФРОВАННОЕ СОЕДИНЕНИЕ МЕЖДУ ВЕБ-СЕРВЕРОМ И ВЕБ-БРАУЗЕРОМ

ЗАЩИТА ОТ DDOS

РЕШАЕТСЯ ЭТОТ ВОПРОС ЕСЛИ ВАШ ХОСТИНГ-ПРОВАЙДЕР ПРЕДОСТАВЛЯЕТ УСЛУГИ ЗАЩИТЫ ОТ DDOS-АТАК ИЛИ ВЫ ПОЛЬЗУЕТЕСЬ УСЛУГАМИ АНТИ-DDOS-СЕРВИСОВ, НАПРИМЕР CLOUDFLARE, DDOS-GUARD, G-CORE LABS, KASPERSKY.

БЕЗОПАСНОСТЬ СТОРОННИХ МОДУЛЕЙ

БОЛЬШИНСТВО ВРЕДОНОСНЫХ АТАК ПРОИСХОДИТ ЧЕРЕЗ СТОРОННИЕ МОДУЛИ. СУТЬ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТОБЫ ИСПОЛЬЗОВАТЬ ФРЕЙМВОРКИ И БИБЛИОТЕКИ СО ВСТРОЕННЫМИ ФУНКЦИЯМИ БЕЗОПАСНОСТИ, КОТОРЫЕ ПОМОГУТ РАЗРАБОТЧИКАМ СВЕСТИ К МИНИМУМУ ПОЯВЛЕНИЕ УЯЗВИМОСТЕЙ В ПРОЦЕССЕ РЕАЛИЗАЦИИ.

SQL-ИНЪЕКЦИИ И XSS-АТАКИ

ЦЕЛЬ ЗЛОУМЫШЛЕННИКОВ АТАКИ SQL-ИНЪЕКЦИЕЙ ЯВЛЯЕТСЯ КОНКРЕТНЫЕ ДАННЫЕ ИЗ БАЗЫ ДАННЫХ И ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫХ XSS-АТАКИ.

ЗАЩИТА ОТ **SQL-**ИНЪЕКЦИЙ И **XSS-**АТАК

SQL-ИНЪЕКЦИИ

- *Аутентификация (должна выполняться по защищенному каналу)*
- *Соединение (в связи с существованием нескольких способов взаимодействия с базой данных посредством службы или API, необходимо обеспечить безопасность соединений с помощью шифрования и аутентификации)*
- *Необходимо избегать нелегитимных входных данных в составе SQL-команд (наилучшим решением является использование параметризованных запросов)*
- *Убедиться в корректной настройке имеющихся средств обеспечения безопасности СУБД и платформы, на которой она установлена.*

XSS-АТАКИ

- *Главной мерой защиты в данном случае является экранирование*
- *Кодирование данных*
- *Проверка uri параметров перед их выполнением*
- *Обязательный urlencode ссылок перед их выполнением*

ЖУРНАЛИРОВАНИЕ И МОНИТОРИНГ

КРОМЕ СТАНДАРТНЫХ СРЕДСТВ ЖУРНАЛИРОВАНИЯ, ПРЕДОСТАВЛЯЕМЫХ ВЕБ-СЕРВЕРОМ, НЕОБХОДИМО УБЕДИТЬСЯ В РЕГИСТРАЦИИ ВРЕМЕНИ СОБЫТИЯ И ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, А ТАКЖЕ ПОТЕНЦИАЛЬНО ОПАСНОЙ АКТИВНОСТИ, ХАРАКТЕРНОЙ ДЛЯ ВАШЕГО ВЕБ-САЙТА. В СЛУЧАЕ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ ВАШЕ ПРИЛОЖЕНИЕ ДОЛЖНО ЗАБЛОКИРОВАТЬ ПОЛЬЗОВАТЕЛЬСКУЮ СЕССИЮ ИЛИ ЗАБЛОКИРОВАТЬ ПО IP-АДРЕСУ, В ОБЩЕМ ПРИНЯТЬ МЕРЫ И СООБЩИТЬ ОБ ЭТОМ АДМИНИСТРАТОРУ.

БЭКАПЫ

РЕГУЛЯРНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ ВЕБ-САЙТА И ВСЕХ ДАННЫХ, ВОЗНИКАЕТ ВОПРОС ГДЕ ХРАНИТЬ ВСЕ ЭТИ ДАННЫЕ С ПОЛНЫМ ОБЕСПЕЧЕНИЕМ КОНФИДЕНЦИАЛЬНОСТИ. ЭФФЕКТИВНЫМ СПОСОБОМ ЯВЛЯЕТСЯ ШИФРОВАНИЕ ХРАНИЛИЩ КРИТИЧНЫХ ДАННЫХ И РЕЗЕРВНЫХ КОПИЙ, А ТАКЖЕ ХРАНЕНИЕ ФАЙЛОВ РЕЗЕРВНЫХ КОПИЙ НЕ НА ФАЙЛОВОЙ СИСТЕМЕ, А В ДРУГОМ МЕСТЕ, В БЕЗОПАСНОСТИ КОТОРОГО НЕТ СОМНЕНИЙ И КОТОРОЕ ВСЕГДА БУДЕТ ПОД РУКОЙ ДЛЯ БЫСТРОГО РАЗВЕРТЫВАНИЯ.

НАДЕЖНОСТЬ ПАРОЛЕЙ

СУЩЕСТВУЕТ ТРИ УРОВНЯ АУТЕНТИФИКАЦИИ И ИСПОЛЬЗОВАНИЕ ТОЛЬКО ПАРОЛЕЙ ОТНОСИТСЯ ЛИШЬ К ПЕРВОМУ – САМОМУ ПРОСТОМУ УРОВНЮ (ВТОРОЙ – МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ; ТРЕТИЙ – АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ШИФРОВАНИЯ).

ЗАЩИТА АДМИНИСТРАТИВНОЙ ПАНЕЛИ

АДМИНИСТРАТИВНАЯ ПАНЕЛЬ ВЕБ-САЙТА, ЯВЛЯЕТСЯ ОДНИМ ИЗ САМЫХ СЛАБЫХ МЕСТ В ОБЩЕЙ СИСТЕМЕ ИЗ-ЗА ОБШИРНОГО ФУНКЦИОНАЛА, СВЯЗАННОГО С ДОБАВЛЕНИЕМ ИЛИ РЕДАКТИРОВАНИЕМ ПОСТОВ И СТРАНИЦ, РАБОТОЙ С ФАЙЛАМИ И МНОГИМ ДРУГИМ. ПОЭТОМУ ВАЖНЫМ УСЛОВИЕМ ЯВЛЯЕТСЯ ОБЕСПЕЧИТЬ НАДЛЕЖАЩИЙ КОНТРОЛЬ ДОСТУПА, А ТАКЖЕ МАКСИМАЛЬНУ. СКРЫТНОСТЬ ОТ ЗЛОУМЫШЛЕННИКОВ МЕСТОНАХОЖДЕНИЯ АДМИНИСТРАТИВНОЙ ПАНЕЛИ, РЕАЛИЗУЕМУЮ ПРОСТЫМ ПЕРЕНОСОМ АДРЕСА НА НЕСТАНДАРТНЫЙ И МАКСИМАЛЬНОЙ ЗАЩИТОЙ ДАННОЙ ТОЧКИ ВХОДА ПОСРЕДСТВОМ ЗАЩИТЫ ОТ ПЕРЕБОРА, ФИЛЬТРАЦИИ ПО IP-АДРЕСАМ И Т.Д.

СПОСОБЫ НАРУШЕНИЯ РАБОТЫ ЭЛЕКТРОННОЙ ПОЧТЫ

- *ЛАВИННАЯ РАССЫЛКА* - СИТУАЦИЯ, КОГДА ЗЛОУМЫШЛЕННИК ПЕРЕГРУЖАЕТ СИСТЕМУ, ОТПРАВЛЯЯ ЕЙ ОГРОМНОЕ ЧИСЛО ПОЧТОВЫХ СООБЩЕНИЙ. СРАВНИТЕЛЬНО НЕСЛОЖНО НАПИСАТЬ КОРОТКУЮ ПРОГРАММУ, КОТОРАЯ ОТПРАВЛЯЕТ МИЛЛИОНЫ ЭЛЕКТРОННЫХ СООБЩЕНИЙ (ВКЛЮЧАЯ ПУСТЫЕ) ВЫБРАННОМУ СЕРВЕРУ С ЦЕЛЬЮ ПАРАЛИЗОВАТЬ ЕГО РАБОТУ. БЕЗ ДОЛЖНОЙ ЗАЩИТЫ СЕРВЕР БУДЕТ ВЫНУЖДЕН ПОСТОЯННО ОТКАЗЫВАТЬ КЛИЕНТАМ В ОБСЛУЖИВАНИИ, ПОСКОЛЬКУ ЕГО ЛОКАЛЬНЫЙ ДИСК БУДЕТ ПЕРЕПОЛНЕН НЕНУЖНЫМИ СООБЩЕНИЯМИ.

- *СПАМ* - РАССЫЛКА ОГРОМНОГО КОЛИЧЕСТВА РЕКЛАМЫ И ИНОЙ ИНФОРМАЦИИ НА ПОЧТОВЫЕ ЯЩИКИ ПОЛЬЗОВАТЕЛЕЙ

- *УТЕЧКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ* - ПРЕЖДЕ ЧЕМ ВАШЕ ПИСЬМО ПОПАДЕТ К ПОЛУЧАТЕЛЮ, ОНО ПРОЙДЕТ ЧЕРЕЗ МНОГО НЕПОДКОНТРОЛЬНЫХ ВАМ СИСТЕМ. ЕСЛИ ВЫ НЕ ЗАШИФРУЕТЕ СВОЕ СООБЩЕНИЕ, ЗЛОУМЫШЛЕННИКИ МОГУТ ПЕРЕХВАТИТЬ И ПРОЧИТАТЬ ЕГО В ЛЮБОЙ ТОЧКЕ МАРШРУТА ПЕРЕСЫЛКИ.

- *ТРОЯНСКИЕ И ВРЕДОНОСНЫЕ ПРОГРАММЫ, ФИШИНГОВЫЕ РАССЫЛКИ*

СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ

- *ПОЧТОВЫЙ АНТИВИРУС - ПРОВОДИТ СКАНИРОВАНИЕ ПИСЕМ НА ПРИСУТСТВИЕ ВРЕДОНОСНОГО ПО*

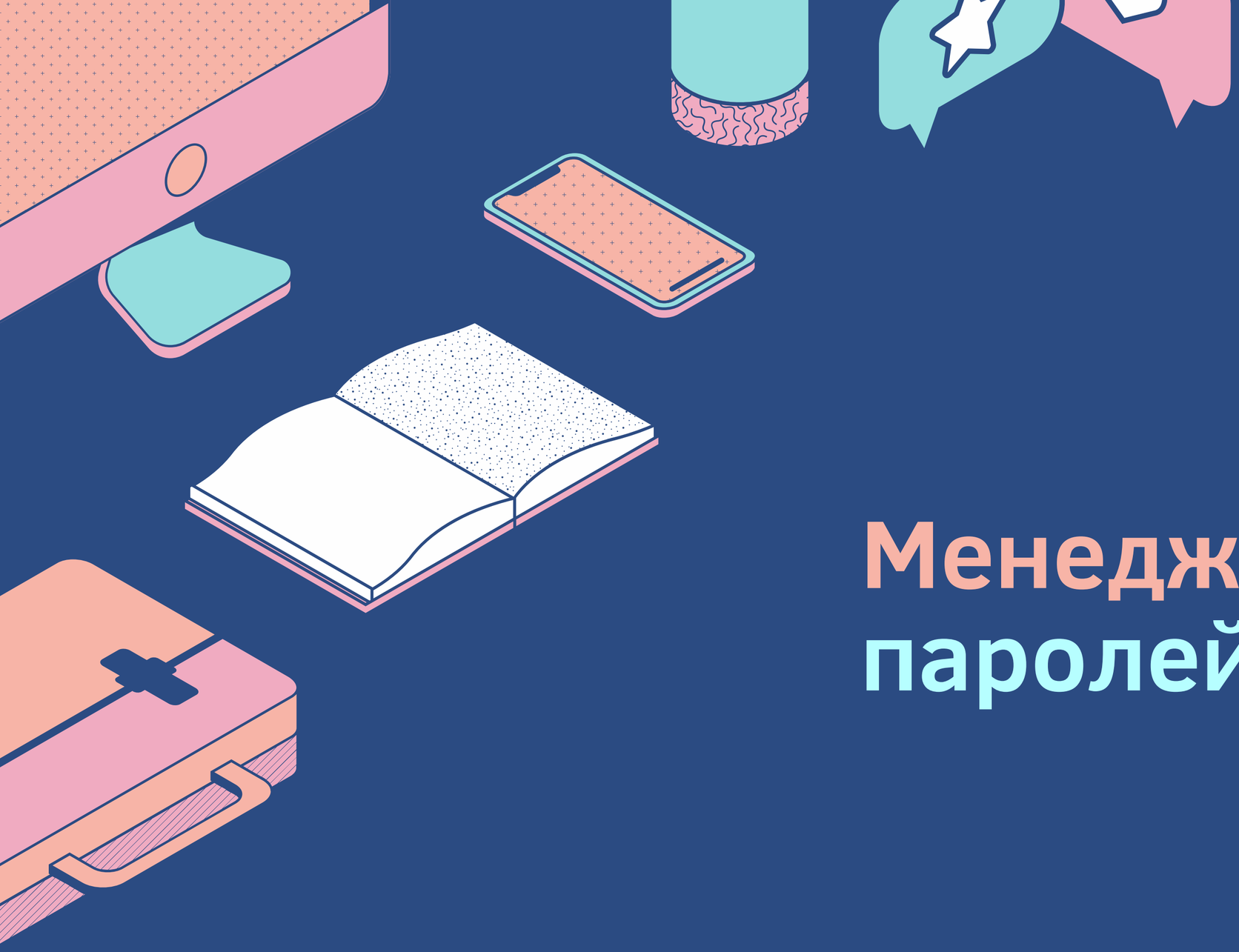
- *АНТИ-СПАМ - ОТВЕЧАЕТ ЗА ВЫЯВЛЕНИЕ РАССЫЛОК*

В ЧАСТНОСТИ ЗАЩИТУ ЭЛЕКТРОННОЙ ПОЧТЫ МОЖНО РАССМАТРИВАТЬ КАК СОВОКУПНОСТЬ СЛЕДУЮЩИХ МЕРОПРИЯТИЙ:

- ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ОТКАЗОУСТОЙЧИВОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ ПОЧТОВЫХ СЕРВЕРОВ.
- УСТАНОВКА СИГНАТУРНОЙ И ПРОАКТИВНОЙ ЗАЩИТЫ ОТ ВИРУСОВ.
- ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ МЕТОДОМ ШИФРОВАНИЯ ИСХОДЯЩИХ СООБЩЕНИЙ С ПОМОЩЬЮ КРИПТОГРАФИЧЕСКИХ ПРОГРАММ.
- ИСПОЛЬЗОВАНИЕ АДАПТИВНОЙ ФИЛЬТРАЦИИ ВХОДЯЩИХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ.
- ЗАЩИТА ОТ DDOS АТАК НА ПОЧТОВЫЕ СЕРВЕРА.
- УСТАНОВКА НАИБОЛЕЕ НАДЕЖНЫХ ПОЧТОВЫХ КЛИЕНТОВ.
- НАСТРОЙКА BLACK/WHITE СПИСКОВ И ПЕРСОНАЛЬНОГО КАРАНТИНА.

В ЦЕЛОМ ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ ТРЕБУЕТ СИСТЕМНОГО ПОДХОДА. ИСПОЛЬЗОВАНИЕ РАЗЛИЧНЫХ РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ ОСНОВЫВАЕТСЯ НА РАБОТЕ КОМПЛЕКСА СПЕЦИАЛИЗИРОВАННЫХ УСТРОЙСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ - ОДНА ИЗ ВАЖНЕЙШИХ КОМПОНЕНТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НКО.

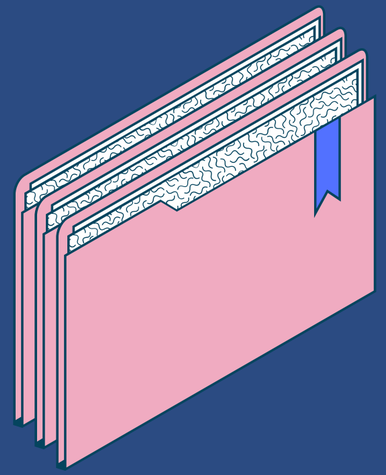
Менеджеры паролей



Что такое менеджер паролей и для чего он нужен?

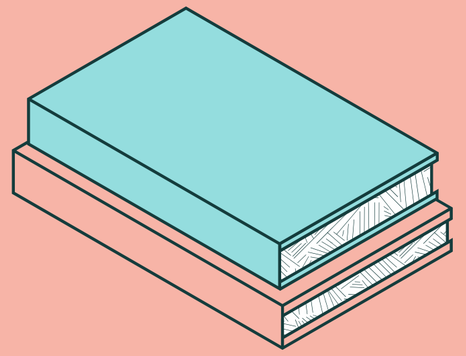
Менеджер паролей – это программа, помогающая пользователям создавать надежные пароли, хранить их в цифровом хранилище, защищенном единым мастер-паролем, а затем по мере необходимости получать их при входе в учетные записи.

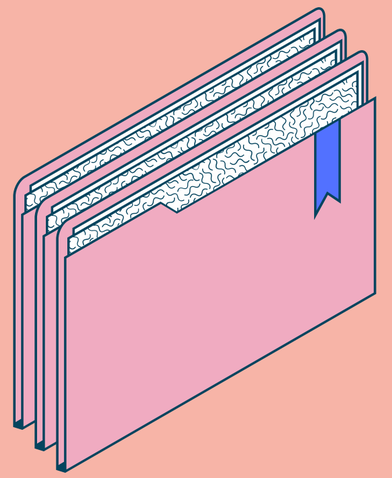
Использование менеджера паролей имеет ряд преимуществ. Утечки паролей – это частое явление, возникающее при взломе веб-сайтов, в результате чего данные пользователей, такие как имена и пароли, попадают в руки злоумышленников. Получив учетные данные для входа в систему, злоумышленники могут использовать их на других веб-сайтах.

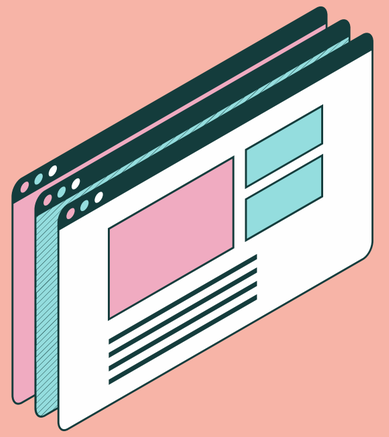


При использовании менеджера паролей все пароли хранятся в одном месте – цифровом хранилище, а мастер-пароль является ключом к этому хранилищу. Мастер-пароль используется для шифрования содержимого хранилища, поэтому он должен быть надежным. Также важно не потерять его, в противном случае придется выполнить сброс паролей для всех онлайн-аккаунтов. Поэтому выбирайте мастер-пароль так, чтобы точно не забыть его. Некоторые менеджеры паролей, используемые на мобильных устройствах, разрешают доступ по отпечатку пальца или распознаванию лица.

Сразу после установки менеджер паролей при каждом входе в приложение или на сайт считывает имя пользователя и пароль и сохраняет их в цифровом хранилище. Надежный менеджер паролей должен отслеживать все изменения, вносимые в имена пользователей и пароли в хранилище.



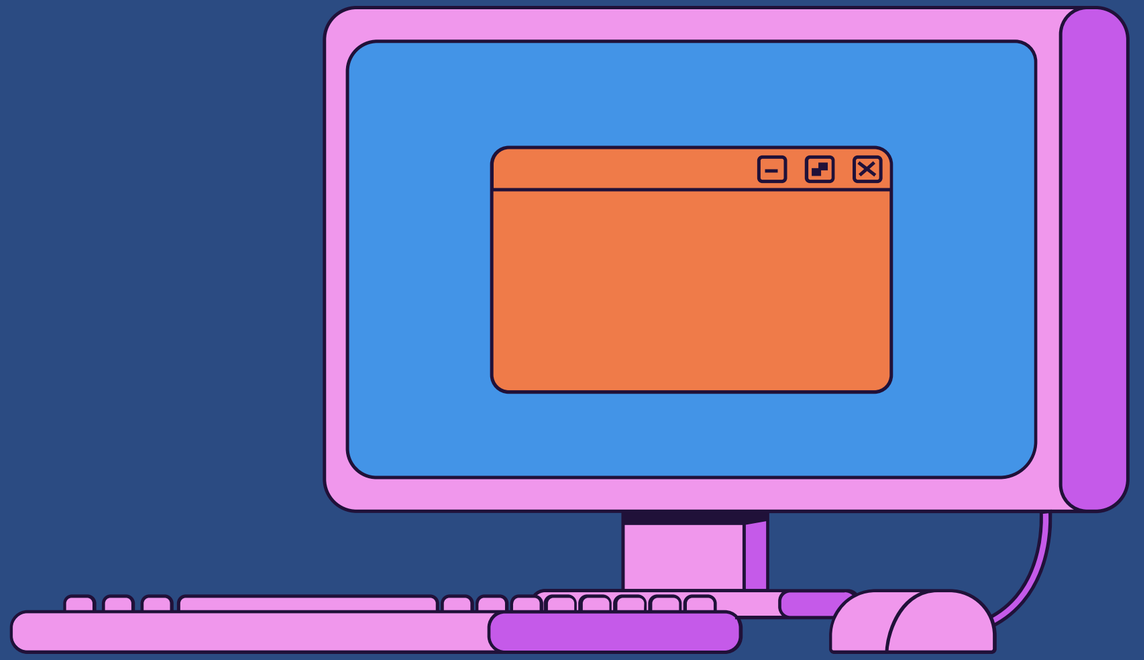




Как работает менеджер паролей?

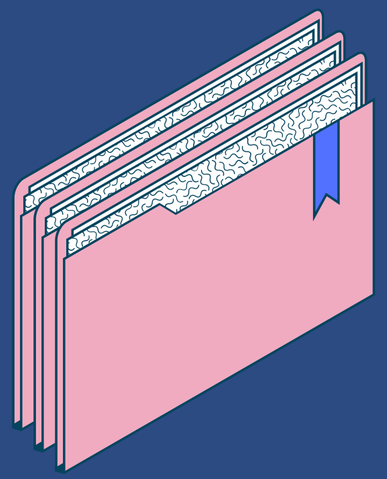
Некоторые менеджеры паролей могут быть взломаны, поэтому важно, чтобы хранимая в них информация была зашифрована. Если менеджер паролей использует являющееся стандартом индустрии шифрование, например, алгоритм Advanced Encryption Standard (AES), у злоумышленников практически не будет возможности расшифровать содержимое.

Менеджеры паролей не хранят и не имеют доступа к мастер-паролю и зашифрованной информации в базе паролей, что обеспечивает дополнительный уровень безопасности. Ключевой аспект безопасности менеджеров паролей заключается в надежности мастер-пароля, поэтому важно использовать сложный пароль и обеспечить его безопасность.



Насколько надежны менеджеры паролей?

Рекомендации по выбору менеджера паролей



1. Выбирайте программу, в которой используется надежное шифрование.

2. Убедитесь, что программа поддерживает функцию блокировки, которая пригодится, если вы забудете пароль.

3. Заранее узнайте, как можно связаться с компанией-поставщиком программы, если возникнут проблемы.

4. Убедитесь, что в программе предусмотрена защита от кражи учетных данных, и выясните, требуется ли предпринимать дополнительные меры для защиты от других видов вредоносной активности.

Менеджеры паролей

МЕНЕДЖЕРОВ ПАРОЛЕЙ СУЩЕСТВУЕТ ОГРОМНОЕ КОЛИЧЕСТВО, НИЖЕ ПРИВЕДЕНА КРАТКАЯ ХАРАКТЕРИСТИКА ОДНИХ ИЗ ПОПУЛЯРНЫХ. У ВСЕХ ПРИВЕДЕННЫХ НИЖЕ МЕНЕДЖЕРОВ ПАРОЛЕЙ ЕСТЬ БЕСПЛАТНАЯ ВЕРСИЯ, ПОЭТОМУ ПРОГРАММУ МОЖНО ОПРОБОВАТЬ, А ОПЛАТИТЬ - ПОЗДНЕЕ

Dashlane

Мониторинг и изменение паролей в один клик.
Поддержка: iOS, Mac, Windows, Android, Web.
Стоимость: 39.99$/год для премиум-аккаунта.

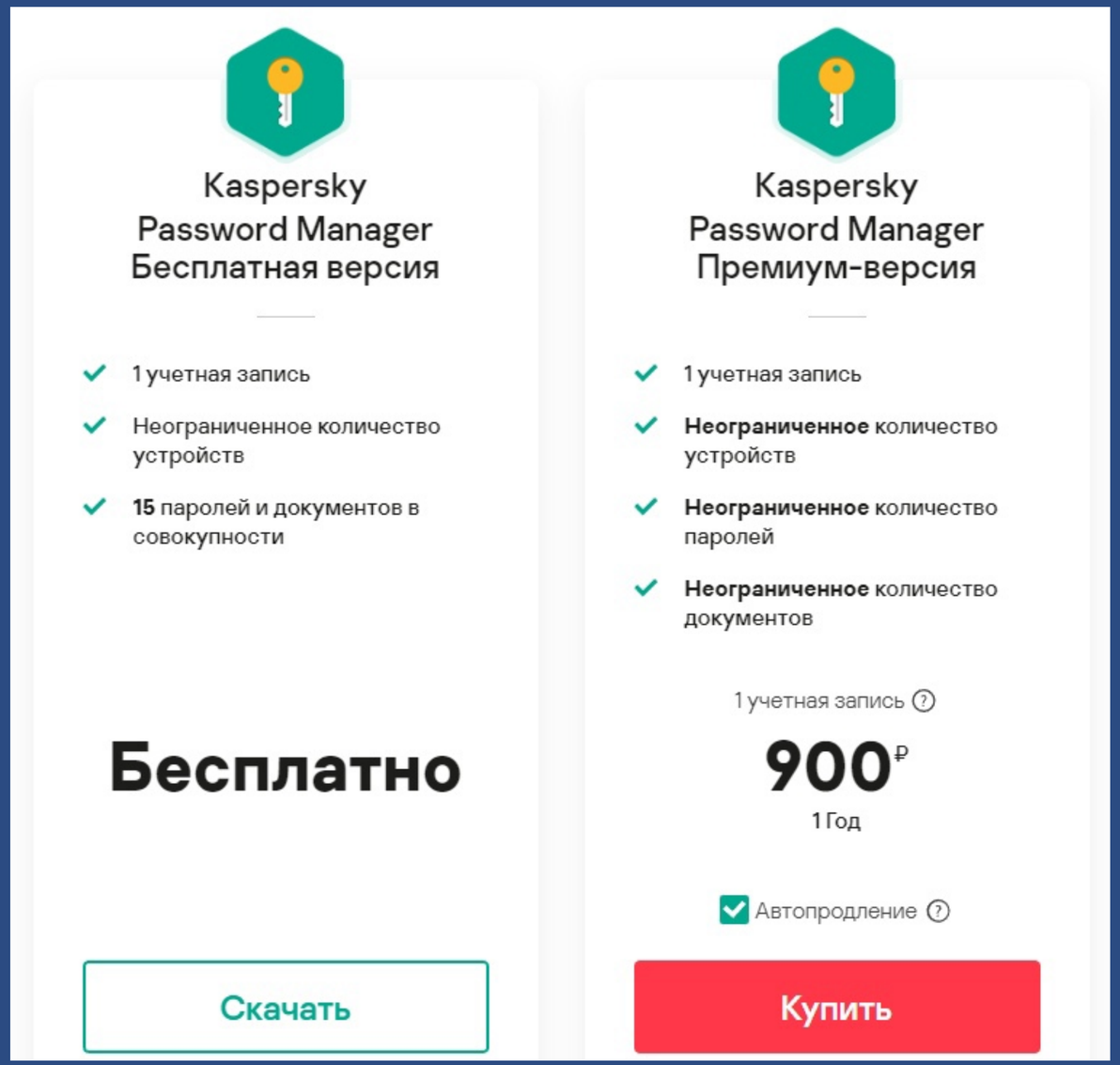
Splikity

Простой инструмент для работы с паролями.
Поддержка: iOS, Chrome, Android, Firefox, Safari.
Стоимость: 4.99$ в месяц или 49.99$ в год.

LastPass

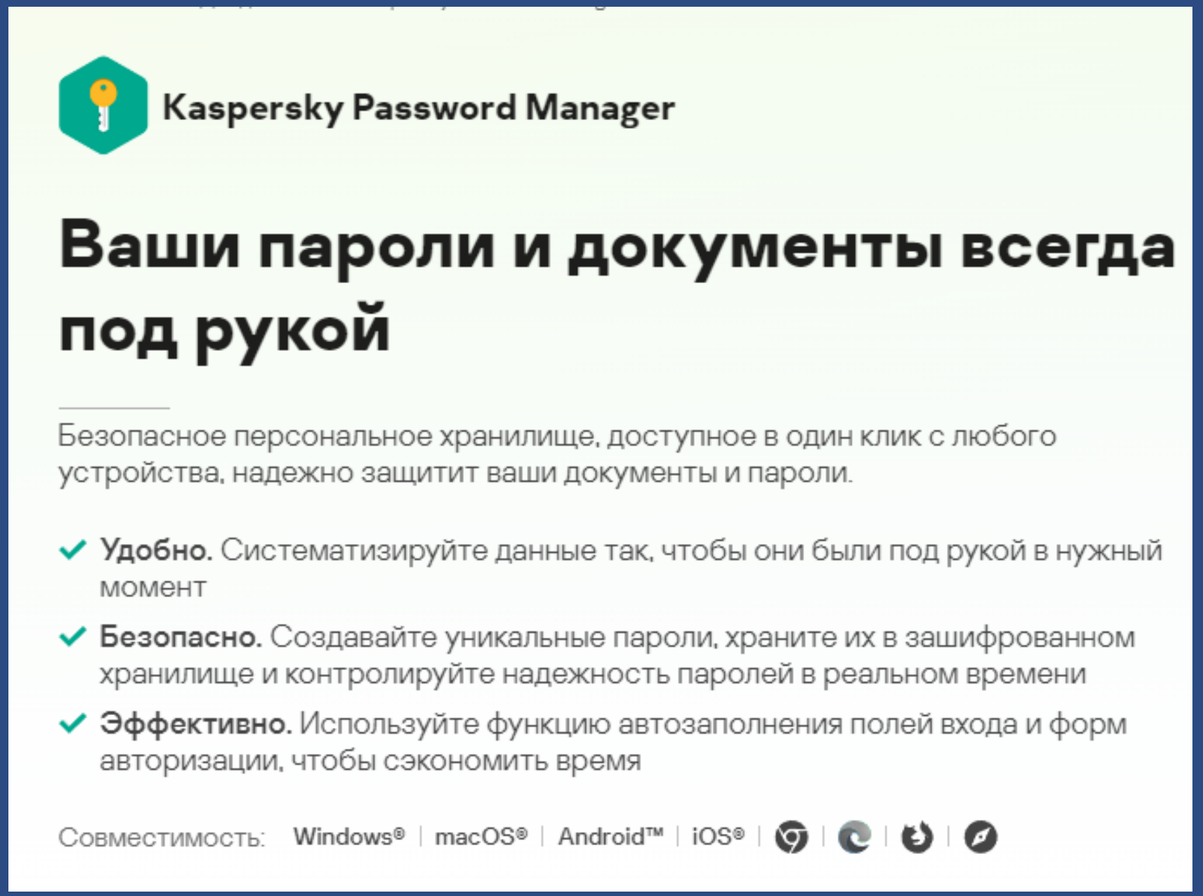
Простой и удобный кросс-платформенный доступ к вашим паролям из любого браузера.
Поддержка: Web, Mac, iOS, Android, Windows.
Стоимость: 12$ в год премиум.

На территории Российской Федерации отличным вариантом для использования будет менеджер паролей от известной компании "Лаборатория Касперского". Как и большинство других менеджеров для защиты здесь используется алгоритм шифрования AES 256 GCM. Сама Лаборатория утверждает, что «злоумышленникам понадобится целая вечность, чтобы взломать его». Одним из безусловных плюсов такого шифрования является возможность получить доступ ко всем пароля с помощью одного мастер-пароля, о котором мы уже писали чуть выше. Ну и, конечно, даже сама компания о ваших паролях ничего не знает. Принцип нулевого разглашения здесь работает.



Из преимуществ Kaspersky Password Manager выделю следующие:

- Kaspersky умеет сохранять не только пароли. (серию и номер паспорта, номера банковских карт и т.д.).
- Все данные можно разделить на папки для лучшего поиска.
- Поддержка клиентов для macOS, iPadOS, iOS и Windows.
- Наличие расширений для Google Chrome, Firefox, Edge и Яндекс.Браузера.
- Возможность входа через биометрию на iPhone или Mac.
- Импорт логинов и паролей из других менеджеров (что нам и нужно).
- Импорт данных из браузера.
- Касперский предлагает неограниченное количество устройств даже в бесплатной версии.



Kaspersky
Password Manager

App Store
★ ★ ★ ★ ★
Глобальный рейтинг: 4,6 из 5

Google Play
★ ★ ★ ★ ★
Глобальный рейтинг: 4,4 из 5

Download it for Windows

Download it for Mac

Download on the App Store

GET IT ON Google Play

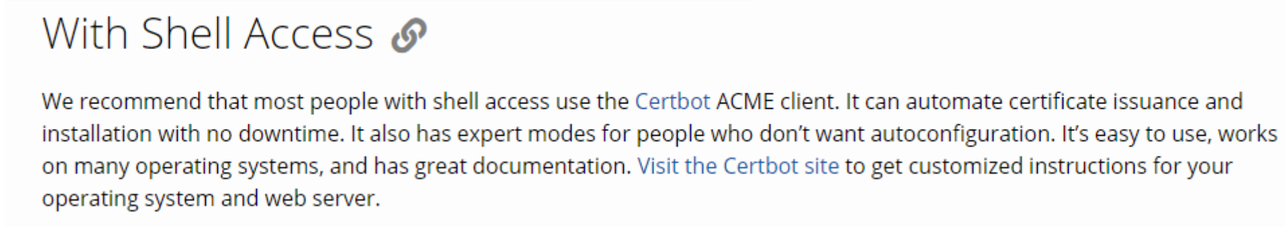
На мобильные устройства Kaspersky Password Manager доступен в Play Market и App Store, а также на официальном сайте kaspersky.ru.

Для установки менеджера паролей с официального сайта требуется:

1. Открыть вкладку "Продукты" в разделе "Для дома" на панели сверху
2. Выбираем необходимую платформу: Windows, MacOS, Iphone, Android
3. Находим Kaspersky Password Manager и нажимаем "Подробнее"
4. Пролистываем страницу до заголовка "Установить Kaspersky Password Manager просто"
5. Загружаем по специальной кнопке и выполняем интуитивно понятные настройки. Для теста работы ограничения в 15 возможных паролей более чем достаточно.

КАК ПОЛУЧИТЬ И НАСТРОИТЬ LET'S ENCRYPT SSL СЕРТИФИКАТ

1. Переходим на сайт Let's Encrypt https://letsencrypt.org
2. Нажимаем Get Started
3. Нажать на Certbot
4. Чтобы получить сертификат, нужно:
   - Иметь свой HTTP веб-сайт
   - Чтобы он был подключен к сети
   - С открытым 80 портом
5. Выбираем используемый HTTP сервер и операционную систему
6. Устанавливаем необходимые пакеты
7. Запускаем CertBot
8. Вводим e-mail
9. Выбираем нужный нам домен
10. Получаем сертификат



СПАСИБО ЗА ВАШЕ ВНИМАНИЕ!