СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 10

Безопасность облачных вычислений

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Основные понятия облачных вычислений
2. Определение безопасности облака
3. Как работает безопасность облака
4. Отличие подходов в обеспечении безопасности облака от традиционных подходов
5. Защита облака
6. Меры обеспечения облачной безопасности

По завершению лекции Вы будете знать:

1. Основные понятия облачных вычислений
2. Определение безопасности облака
3. Работу безопасности облака
4. Отличие подходов в обеспечении безопасности облака от традиционных подходов
5. Защиту облака
6. Меры обеспечения облачной безопасности

Основные понятия облачных вычислений

Облачные вычисления (CC, cloud computing) – это технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис.

- **Инфраструктура как сервис** – это предоставление компьютерной инфраструктуры как услуги на основе концепции облачных вычислений.
- **Платформа как сервис** – это предоставление интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений как услуги.
- **Программное обеспечение как сервис** – модель развертывания приложения, которая подразумевает предоставление приложения конечному пользователю как услуги по требованию. Доступ к такому приложению осуществляется посредством сети, а чаще всего посредством Интернет-браузера.
- **Частное облако** – это вариант локальной реализации «облачной концепции», когда компания создает ее для себя самой, в рамках одной организации.
- **Публичное облако** – используется облачными провайдерами для предоставления сервисов внешним заказчикам.
- **Распределенные вычисления** – технология когда большая ресурсоёмкая вычислительная задача распределяется для выполнения между множеством компьютеров, объединённых в мощный вычислительный кластер сетью или интернетом.

Определение безопасности облака

Безопасность облака – это раздел кибербезопасности, посвященный защите облачных вычислительных систем. Сюда входит защита конфиденциальности и данных во всех объектах сетевой инфраструктуры, онлайн-приложениях и платформах. Участвовать в этом должны как поставщики облачных услуг, так и пользователи, будь то частные лица, малые и средние предприятия или корпорации.

Облачные службы размещаются на серверах с постоянным подключением к интернету. Поставщики рассчитывают на доверие пользователей, поэтому в их интересах обеспечивать неприкосновенность хранящихся в облаке личных данных. Тем не менее облачная безопасность отчасти находится в руках самих пользователей. Для надежной защиты важно, чтобы обе стороны понимали свою ответственность.

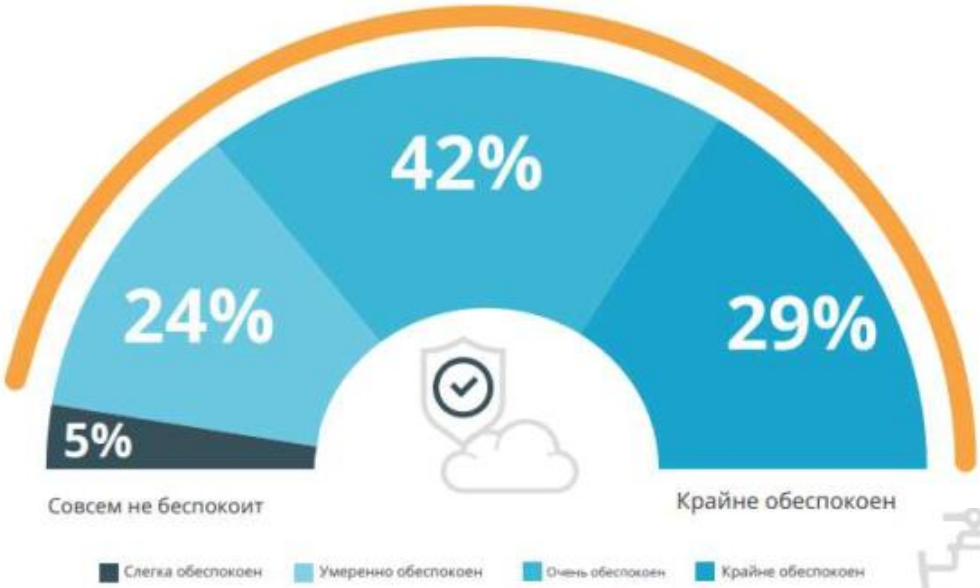
Безопасность облака – это совокупность категорий:

- безопасность данных;
- управление идентификацией и доступом;
- административный контроль (политика предотвращения, обнаружения и устранения угроз);
- планирование хранения данных и обеспечения непрерывности бизнеса;
- соблюдение нормативно-правовых требований.

На первый взгляд может показаться, что для обеспечения безопасности в облаке подходят те же методы, что и в традиционных IT-средах, но это не так.

Определение безопасности облака

95% организаций обеспокоены облачной безопасностью



67%

Риск потери и утечки данных

61%

Угрозы конфиденциальности данных

49%

Случайное раскрытие учетных данных

Определение безопасности облака

Безопасность облака включает в себя набор технологий, протоколов и наработок для защиты облачных сред, приложений и данных. Для начала необходимо понять, что именно нужно защищать и какие аспекты систем требуют управления.

В целом борьба с уязвимостями происходит преимущественно на серверной стороне: это обязанность поставщика облачных услуг. Но и у клиентов есть свои обязанности, помимо выбора надежного поставщика. Клиенты должны правильно использовать настройки защиты, уметь безопасно пользоваться службами, а также заботиться о защите всех устройств и сетей конечных пользователей.

Независимо от уровня ответственности все меры безопасности облака направлены на защиту следующих компонентов:

- **физические сети** – маршрутизаторы, электросети, кабели, системы кондиционирования воздуха и др.;
- **носители данных** – жесткие диски и др.;
- **серверы данных** – аппаратное и программное обеспечение опорной сети;
- **сети виртуализации** – ПО для виртуальных машин, хост-компьютеры, гостевые виртуальные машины;
- **операционные системы** – программное обеспечение, на которое устанавливаются все остальные программы;
- **связующие программы** – ПО для управления интерфейсами программирования приложений;
- **среды выполнения** – средства запуска и поддержания работы программ;
- **данные** – вся информация, которая хранится, изменяется и предоставляется пользователям;
- **приложения** – традиционные программные сервисы (электронная почта, налоговое ПО, офисные приложения и др.);
- **оборудование конечного пользователя** – компьютеры, мобильные устройства, устройства интернета вещей и др.

Определение безопасности облака

Что вы считаете самой большой угрозой безопасности в публичных облаках?

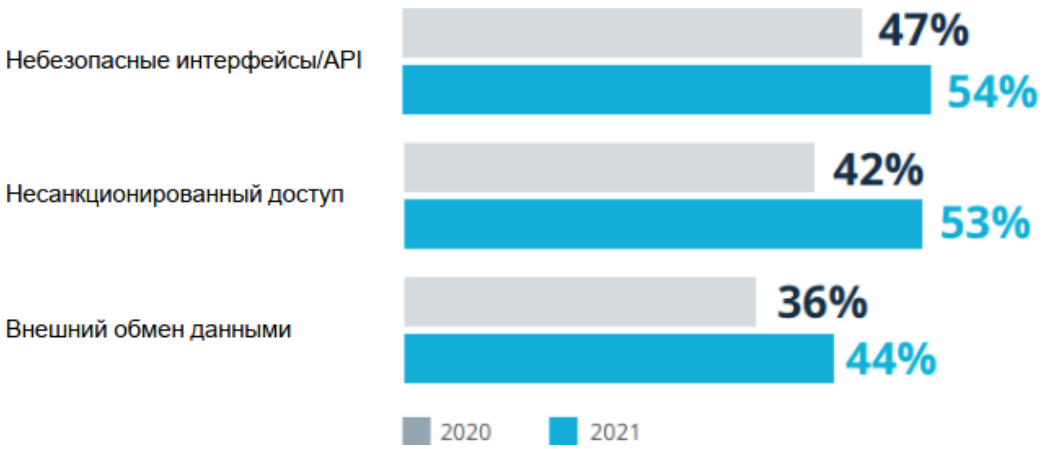
71%

Неправильная конфигурация облачной платформы/неправильная настройка

Рост на 22% по сравнению с прошлым годом

59%

Эксфильтрация конфиденциальных данных



Угрозы

- Утечки данных
- Неверная конфигурация и недостаточный контроль изменений
- Отсутствие паттерн безопасной архитектуры и стратегии облачной безопасности.
- Недостаточная уровень контроля управлением идентификацией, учетными данными, доступом и ключами
- Взлом аккаунта
- Внутренние угрозы – угрозы утечки информации
- Небезопасные интерфейсы взаимодействия и API
- Непрозрачность использования облачных сервисов - Shadow IT (Ограниченная видимость использования облачных служб)
- Злоупотребление и неправомерное использование облачных сервисов
- Слабый контроль управления облачной инфраструктурой

Определение безопасности облака

В случае облачных технологий не всегда легко определить, кто несет ответственность за каждый из этих компонентов, в результате чего размываются соответствующие обязанности клиентов. Поскольку процесс защиты облака зависит от того, кто за какие компоненты отвечает, важно понимать принцип классификации этих компонентов.

Для простоты компоненты облачных систем можно разделить на две основные группы.

1. Облачные службы разных типов предоставляются сторонними поставщиками в виде модулей, из которых складывается облачная среда. В зависимости от типа службы может требоваться управление разными компонентами, составляющими ту или иную службу.

- **В любой сторонней облачной службе** поставщик управляет физической сетью, хранилищем данных, серверами и системами виртуализации. Служба размещается на серверах поставщика и посредством виртуализации предоставляется клиентам для удаленного доступа. Таким образом поставщик экономит на оборудовании и инфраструктуре, а пользователи получают доступ к необходимым вычислительным возможностям через интернет;
- Облачные службы **Software-as-a-Service (программное обеспечение как услуга, SaaS)** дают пользователям доступ к приложениям, которые просто хранятся и запускаются на серверах поставщика. Поставщик управляет приложениями, данными, средой выполнения, связующими программами и операционной системой. Клиентам остается лишь получить доступ к своим приложениям. *Примеры SaaS: Google Диск, Slack, Salesforce, Microsoft 365, Cisco WebEx, Evernote*;
- Облачные службы **Platform-as-a-Service (платформа как услуга, PaaS)** позволяют клиенту разрабатывать свои приложения, которые запускаются в его собственной «песочнице» на сервере поставщика. Поставщик управляет средой выполнения, связующими программами и операционной системой. Клиенты самостоятельно управляют своими приложениями, данными, пользовательским доступом, устройствами и сетями конечных пользователей. *Примеры PaaS: Google App Engine, Windows Azure*;

Определение безопасности облака

- Облачные службы **Infrastructure-as-a-Service (инфраструктура как услуга, IaaS)**– это оборудование и возможности удаленного подключения, позволяющие клиентам размещать в облаке все их вычислительные ресурсы, вплоть до операционной системы. Поставщик управляет только основными облачными службами. Клиенты отвечают за операционную систему и все, что на ней устанавливается, включая приложения, данные, среды выполнения и связующие программы. Они также управляют пользовательским доступом, устройствами и сетями конечных пользователей. *ПримерыIaaS: Microsoft Azure, Google Compute Engine (GCE), Amazon Web Services (AWS).*

2. Облачные среды представляют собой такие модели развертывания, в которых при помощи одной или нескольких облачных служб создается система для конечных пользователей и организаций. Таким образом обязанности по управлению (в том числе обеспечение безопасности) разделяются между клиентами и поставщиками.

На данный момент используются следующие облачные среды:

- **Публичные облачные среды** состоят из облачных служб, предназначенных для нескольких арендаторов. В таких средах несколько клиентов делят между собой серверы одного поставщика, наподобие аренды офисного здания в бизнес-центре. Доступ к этим сторонним службам под управлением поставщика предоставляется через веб-интерфейс.
- В **частных сторонних облачных средах** поставщик предоставляет клиенту собственное облако в исключительное пользование. Это среды, предназначенные для одного арендатора, которые, как правило, находятся в собственности, под контролем и удаленным управлением внешнего поставщика.
- **Частные внутренние облачные среды** также состоят из облачных серверов, рассчитанных на одного арендатора, но управляются из собственного центра обработки данных. В этом случае компания сама управляет облачной средой, контролируя все настройки и установку каждого элемента.
- **Многооблачные среды** предполагают использование двух и более облачных служб от разных поставщиков, при этом облака могут быть публичными, частными или смешанными.
- **Гибридные облачные среды** – это комбинация частного стороннего облака и (или) локального частного облачного центра обработки данных с одной или несколькими публичными облачными службами.

Как работает безопасность облака

Каждая мера для облачной безопасности нацелена на выполнение одной или нескольких следующих задач:

- ❑ восстановление данных в случае их утери;
- ❑ защита хранилищ данных и сетей от кражи данных;
- ❑ предотвращение человеческих ошибок и небрежности, приводящих к утечке данных;
- ❑ сокращение последствий любого взлома данных или системы.

Безопасность данных – это аспект облачной безопасности, связанный с технической стороной предотвращения угроз. Технологии позволяют поставщикам и клиентам делать конфиденциальные данные невидимыми и недоступными. Самая мощная из доступных технологий такого рода – *шифрование*. Шифрование делает ваши данные полностью нечитаемыми, и восстановить их сможет только тот, у кого есть ключ шифрования. Даже если ваши зашифрованные данные будут украдены, воспользоваться ими не получится. В облачных сетях также важны *средства защиты передаваемых данных*, такие как виртуальные частные сети (VPN).

Управление идентификацией и доступом (IAM) связано с правами доступа, предоставляемым пользователям. Сюда также относится управление аутентификацией и авторизацией учетных записей. *Контроль доступа* позволяет ограничить пользователям доступ к закрытым данным и системам и распространяется как на проверенных пользователей, так и на потенциальных злоумышленников. Управление паролями, многофакторная аутентификация – эти и другие методы защиты относятся к IAM.

Как работает безопасность облака

Административный контроль сосредоточен на политике предотвращения, обнаружения и устранения угроз. Такие подходы, как *анализ угроз*, могут помочь предприятиям разных размеров в отслеживании и приоритизации угроз, чтобы защитить важнейшие системы. Индивидуальным клиентам тоже не помешает *знать, как безопасно пользоваться облачными службами*. Обычно это касается организаций, однако правила безопасного пользования системой и реагирования на угрозы пригодятся любому пользователю.

Планирование хранения данных и обеспечения непрерывности бизнеса включает меры восстановления утерянных данных в случае технического сбоя. При планировании опираются на методы *дублирования информации*, например на создание резервных копий. Кроме того, не помешают технические средства обеспечения бесперебойной работы. Хороший план обеспечения непрерывности бизнеса должен также включать *проверку действительности резервных копий* и подробные инструкции по восстановлению данных для сотрудников.

Соблюдение нормативно-правовых требований гарантирует защиту конфиденциальных данных пользователей в соответствии с законом. Государство заботится о том, чтобы личные данные людей не использовались в коммерческих целях, обязывая организации соблюдать установленные требования, например *маскировать данные*, то есть использовать шифрование для скрытия личности пользователя.

Отличие подходов в обеспечении безопасности облака от традиционных подходов

С переходом на облачные вычисления традиционный подход к IT-безопасности претерпел огромные изменения. Облачные среды удобнее, однако постоянное подключение к интернету требует новых мер безопасности. Безопасность облака как более современное решение в сфере кибербезопасности отличается от традиционных подходов рядом аспектов.

Хранение данных. Главное отличие в том, что более ранние модели IT полагались на локальное хранение данных. Тем не менее, несмотря на возможность полноценного контроля безопасности, локальные IT-платформы дороги и не отличаются гибкостью. Облачные платформы помогают сэкономить на разработке и эксплуатации систем, но при этом частично лишают пользователей контроля.

Скорость масштабирования. Аналогичным образом безопасность облака требует особого внимания при масштабировании корпоративных IT-систем. В облаке используется модульная инфраструктура и приложения с возможностью быстрой мобилизации. Это облегчает адаптацию системы к организационным переменам, однако, вследствие потребности организации в постоянных обновлениях и повышении удобства работы, постоянно приходится задумываться об уровне безопасности.

Отличие подходов в обеспечении безопасности облака от традиционных подходов

Взаимодействие с системой конечного пользователя. Облачные системы взаимодействуют со многими другими системами и службами, которые также необходимо защищать, причем это справедливо как для организаций, так и для индивидуальных пользователей. Необходимо управление правами доступа на всех уровнях: на устройствах конечных пользователей, для ПО и даже в сети. Кроме того, поставщикам и пользователям нужно отслеживать уязвимости, возникающие из-за небезопасных установки приложений и доступа к системам.

Близость к другим данным и системам в сети. Постоянная связь между облаком и пользователями создает угрозу даже для поставщика облачных услуг. В сетевой среде один единственный уязвимый компонент может стать брешью для компрометации всей системы. Предоставляя клиентам услуги, включая хранение данных, поставщики облачных услуг постоянно подвергаются опасности. Сохраняя данные на собственные системы вместо систем конечных пользователей, поставщики вынуждены принимать дополнительные меры безопасности.

Для решения большинства проблем облачной безопасности – как в персональной, так и в деловой среде – требуется проактивное участие и клиентов, и поставщиков. Это означает, что и те и другие равным образом должны уделять внимание:

- безопасной настройке и обслуживанию систем;
- обучению пользователей безопасному поведению и техническим мерам безопасности.

Риски для безопасности облака

От знания рисков зависит, какие меры безопасности будут приниматься. Незащищенная облачная среда подвергает пользователей и поставщиков всем видам киберугроз:

- **риски облачной инфраструктуры**, включая несовместимые устаревшие системы и сбои в сторонних услугах хранения данных;
- **внутренние угрозы из-за человеческого фактора**, например неверной настройки пользовательского доступа;
- **внешние угрозы**, почти всегда связанные с действиями злоумышленников, например атаки вредоносных программ, фишинговые и DDoS-атаки;

Для облака главным риском является отсутствие периметра. Традиционная киберзащита в первую очередь направлена на обеспечение безопасности периметра, но облачные среды очень тесно взаимосвязаны, а значит, небезопасные API (интерфейсы программирования приложений) и кража учетных записей представляют серьезную опасность. Учитывая специфику рисков, специалисты по кибербезопасности теперь должны делать упор именно на контроль данных.

Взаимосвязанность также представляет проблему для сетей. Часто преступники проникают в сеть через взломанную или незащищенную учетную запись. Если злоумышленник получит доступ к облаку, он сможет воспользоваться его плохо защищенными интерфейсами, чтобы заполучить нужные данные из различных баз данных или узлов. Более того, он даже может использовать свои собственные облачные серверы для экспортирования и хранения похищенных данных. Система безопасности должна защищать все облако, а не только хранящиеся в нем личные данные.

Сторонние услуги хранения данных и онлайн-доступ также представляют угрозу. Если в работе какой-либо службы произойдет сбой, вы не сможете получить доступ к своим файлам. Например, в случае перегрузки мобильной сети вы можете в самый неподходящий момент оказаться без доступа к облаку. Или отключение электроэнергии может затронуть центр обработки данных, в котором хранятся ваши данные, и даже привести к их безвозвратной потере.

Защита облака

Шифрование – один из лучших способов защитить облачные системы. Варианты шифрования, которые могут предложить как поставщик облачных услуг, так и сторонний поставщик защитных решений для облачных сред:

- **шифрование всех сообщений** в облаке;
- **шифрование особо секретных данных**, таких как учетные данные;
- **сквозное шифрование** всех загружаемых в облако данных.

Наибольшему риску перехвата данные подвергаются во время перемещения – из одного хранилища в другое или из облака в ваше локальное приложение. Таким образом, сквозное шифрование лучше всего гарантирует безопасность критичных данных в облаке: не имея ключа, посторонние никогда не смогут прочесть ваши сообщения.

Самостоятельное шифрование данных перед их отправкой в облако или использование облачной службы, которая предоставляет такую услугу. Если облако используется только для хранения не конфиденциальных данных, например рекламных роликов компании, использование сквозного шифрования будет явным перебором. Однако, если речь идет о конфиденциальной финансовой или бизнес-информации, сквозное шифрование просто необходимо.

Если используется шифрование, необходимо учитывать о важности безопасного хранения ваших ключей. Требуется хранить резервную копию ключа (желательно не в облаке). Также имеет смысл регулярно менять ключи шифрования.

Защита облака

Конфигурация – мощное средство в арсенале защиты облака. Часто взлом облака происходит из-за такой элементарной уязвимости, как ошибка конфигурации. Необходимо исключить такие ошибки, и риск утечки данных из облака станет гораздо меньше:

- **нельзя использовать настройки по умолчанию**. Так открывается возможность проникновения в систему;
- **нельзя оставлять открытым контейнер облачного хранилища.** Так появляется возможность просмотра содержимого контейнера, просто открыв его URL-адрес;
- **если поставщик облачных услуг предоставляет возможности безопасности, которые можно включить,** необходимо использовать их. Игнорируя доступные возможности, повышается риск подверженности атакам.

***Элементарные принципы кибербезопасности*.**

- **Использование надежных паролей**. Пароли, включающие сочетания букв, цифр и специальных символов, будет сложнее взломать. необходимо избегать очевидных замен (таких как замена буквы S символом $). Случайный набор символов – лучший вариант.

Защита облака

- **Использование менеджера паролей** – он позволит создать для каждого приложения, набора данных и службы индивидуальные пароли, которые не нужно будет запоминать. Однако в этом случае очень важно защитить надежным мастер-паролем сам менеджер.
- **Регулярные резервные копии**, чтобы в случае недоступности облачной службы или потери данных на стороне поставщика вы могли полностью восстановить информацию. Резервные копии могут храниться на вашем домашнем компьютере, на внешнем жестком диске или даже в другом облаке, если вы уверены, что эти два поставщика облачных услуг не используют одну и ту же инфраструктуру.
- Необходимо **менять разрешения**, чтобы никакие пользователи и устройства не могли получить доступ к данным, если только в этом не будет необходимости. Компании могут обеспечить это посредством настроек разрешений базы данных.
- **Защита антивирусом или комплексным защитным решением.**
- **Нельзя осуществлять доступ к данным через публичные сети Wi-Fi**, особенно при отсутствии надежного механизма аутентификации. Необходимо использовать виртуальную частную сеть (VPN) для защиты подключения к облаку.

Защита облака

Решения для безопасности гибридных облачных сред

Службы безопасности гибридных облачных сред могут стать разумным выбором для бизнес-клиентов. Они больше подходят для бизнеса, потому что они, как правило, слишком сложны для персонального пользования. Сочетание масштабируемости и доступности облака с локальным контролем определенных данных – это то, что нужно малым и средним предприятиям и корпорациям.

Преимущества гибридных облачных сред с точки зрения безопасности.

Сегментация служб позволяет организации контролировать хранение данных и доступ к ним. Например, можно создать несколько уровней безопасности, загрузив основные данные, приложения и процессы в облако и оставив наиболее конфиденциальную информацию под локальным контролем. Кроме того, разделение данных поможет организации соблюсти правовые положения о защите информации.

Избыточность – еще одно преимущество гибридных облачных сред. Можно перенести повседневную деятельность в публичное облако и создавать резервные копии систем на локальных серверах. Так работа будет продолжена даже в случае потери соединения с одним из центров обработки данных или его заражения программой-вымогателем.

Меры обеспечения облачной безопасности

1. Изучение модели совместной ответственности
2. Знакомство с поставщиком облачных услуг
3. Управление идентификацией и доступом к облачным ресурсам
4. Обучение персонала
5. Формулирование и установка политики облачной безопасности
6. Защита и контроль периметра и конечных точкек
7. Шифрование данных в движении и в состоянии покоя
8. Внедрение практики DevSecOps (разработка, безопасность и операции)
9. Управление конфиденциальными сведениями
10. Управление рисками облаков
11. Проведение оценки соответствия требованиям законодательства
12. Разработка планов непрерывности и восстановления совместно с поставщиком облачных услуг
13. Проведение аудитов и тестов на проникновение (пентестинга)