Nagoev Zalimhan Vyacheslavovich – e-mail: zaliman@mail.ru; phone: +78662426552; cand. of eng. sc.; head of the department of multiagent systems.

Makarevich Oleg Borisovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: mak@sfedu.ru; 2, Chekhov street, build. "I", Taganrog, Russia; phone: +78634312018; the department of security in data processing technologies; head of department; dr. of eng. sc.

УДК 004.75

О.Ю. Пескова, К.Е. Степовая

ОСОБЕННОСТИ АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ*

Приведена классификация облачных сервисов. Показаны группы требований к облачным системам. Описаны референтная архитектура облачных вычислений NIS, модели сервиса и развертывания облачных систем, представленные в данной модели. Рассмотрены основные проблемы обеспечения безопасности в облачных сервисах. Предложена классификация проблем информационной безопасности облачных технологий. Перечислены организации, занимающиеся вопросами стандартизации обеспечения безопасности облачных систем. Разработан перечень требований к обеспечению безопасности для различных классов облачных систем по следующим направлениям: Классификация и управление активами, Вопросы безопасности, связанные с персоналом, Физическая защита ЦОД, Управление передачей данных и операционной деятельностью, Контроль доступа, Мониторинг доступа и использования системы, Разработка и обслуживание систем, Меры по обеспечению непрерывной работы системы, Соответствие требованиям. По каждому требованию в рамках разрабатываемой методики конкретизированы следующие вопросы: Модель развертывания, для которой данный критерий критичен, Цель применения рекомендаций, Угрозы, которые могут быть ликвидированы при применении данных рекомендаций.

Облачные системы; защищенность; требования к обеспечению безопасности.

O.Y. Peskova, K.E. Stepovaja

FEATURES OF THE ANALYSIS OF INFORMATION SECURITY OF CLOUDY SYSTEMS

The paper provides a classification of cloud services, groups of requirements to cloudy systems are shown, and describes the architecture of cloud computing of NIS, model of service and the expansions of cloudy systems presented in this model. The main problems of ensuring safety in cloudy services are considered. Classification of problems of information security of cloudy technologies is offered. Lists the organizations dealing with issues of standardization of safety of cloudy systems. A list of requirements to safety is developed for various classes of cloudy systems in the following directions: Classification and asset management, Safety issues related with the personnel, Physical protection of data center, Management of data transmission and operational activity, Access control, Monitoring of access, Development and maintenance of systems, Measures for ensuring continuous work of system, Compliance to requirements. According to each requirement within a developed methodology the following questions are specified: Deployment model for which this criterion is critical, Objective application of recommendations, Threats can be eliminated by the application of these recommendations.

Cloud systems; security; safety requirements.

* Работа поддержана грантом РФФИ 13-07-00244-а.

1. Требования к облачным сервисам. Облачные сервисы все активнее используются пользователями для своих личных и рабочих целей. Например, многие уже не представляют эффективной работы без облачных хранилищ данных (dropbox, google drive и многие другие), используя их не только для хранения копий файлов но и для реализации простых, но при этом достаточно эффективных схем совместной работы с документами. Для людей, чья жизнь и работа связаны с обработкой большого объема информации, мощным инструментом стали облачные системы работы сданными (одним из наиболее функциональных сервисов среди подобных систем можно назвать Evernote). При этом даже для частных лиц вопросы обеспечения безопасности важны и во многом влияют на выбор конкретных поставщиков услуг. В последние годы многие организации тоже задумываются над возможностью перевода (полностью или частично) технологической цепочки обработки информации в облака, и для них вопросы защиты целостности и конфиденциальности данных (а также надежности системы в целом) выходят на первое место.

По ряду опросов, проведенных в западных компаниях, от 35 до 75 % организаций используют облачные технологии в том или ином виде, причем до 70 % из них используют больше одного облака. По данным прошлогоднего отчета State of the Cloud компании RightScale, 33 % опрошенных отметили, что основным предметом беспокойства при принятии решения об использовании облака была безопасность; сейчас этот показатель снизился почти вдвое, до 18 % [1].

Тем не менее, до сих пор еще нет четкого и однозначного определения, какие системы относятся к облачным. В 2008 году был опубликован документ IEEE «ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing» [2], в котором дается следующее определение (приведем наиболее распространенный перевод): «Облачная обработка данных – это парадигма, в рамках которой информация постоянно хранится на серверах в интернет и временно кэшируется на клиентской стороне, например, на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т.д.». Это определение слишком обобщено, поэтому нуждается в дополнительных уточнениях.

Чаще всего говорят о следующем наборе требований к облачным системам:

1. Сетевой доступ к сервисам обеспечивается с использованием стандартных протоколов –обычных и защищенных (*универсальность доступа*).
2. Объем предоставляемых услуг зависит от потребностей клиента (равно как и от его возможностей), при этом объем и перечень предоставленных услуг может быть изменен клиентом самостоятельно, в идеале без специальных обращений к провайдеру услуг (*самообслуживание по требованию и эластичность услуг*).
3. Оборудование, обеспечивающее обработку и хранение данных, не выделяется целиком и полностью под отдельного клиента, а обеспечивает работу пула клиентов, перераспределяя мощности с учетом их текущих потребностей (*объединение ресурсов*).
4. К оборудованию и технологическим процессам обработки данных предъявляются значительно более жесткие требования с точки зрения надежности и отказоустойчивости (*высокий уровень доступности, низкие риски неработоспособности*).

2. Требования к облачным сервисам. Свои рекомендации по организации облачных вычислений предложил National Institute of Standarts and Technology (NIST) [3], [4]. Референтная (эталонная) архитектура облачных вычислений NIST (рис. 1, [4]) представляет:

- три модели сервиса (Программное обеспечение как услуга -Software as a Service (SaaS), Платформа как услуга – Platform as a service (PaaS), Инфраструктура как услуга – Infrastructure as a Service (IaaS));
- четыре модели развертывания (частное облако – private cloud, общее облако – community cloud, публичное облако – public cloud, гибридное облако – hybrid cloud);
- пять основных характеристик (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service).

В данной архитектуре представлены 3 типа моделей сервиса:

1. IaaS (Infrastructure as a service - Инфраструктура как сервис/услуга).

Пользователь арендует инфраструктуру в целом, а не конкретный набор услуг, т.е виртуальный сервер с адресом или набором адресов и часть системы хранения данных. Управление службой осуществляется через специальный интерфейс (API). Клиент может устанавливать и запускать любое ПО, от операционных систем до прикладных сервисов. Кроме того, клиент может управлять частью сетевых сервисов (например, межсетевым экраном).

2. PaaS (Platform as a service – Платформа как сервис/услуга).

PaaS – это модель, при которой пользователю предоставляется установленная, настроенная и готовая к работе виртуальная платформа из одного или нескольких виртуальных серверов с операционными системами и специализированными приложениями. Клиенты могут устанавливать на этой платформе приложения – как собственные, так и сторонней разработки. Часто в состав платформы входят средства разработки и тестирования ПО.

3. SaaS (Software as a service – Программное обеспечение как сервис/услуга).

Облачные решения SaaS позволяет удалённо пользоваться программным обеспечением провайдера с использованием различных клиентов. Поставщик разрабатывает приложение или набор приложений и предоставляет доступ к нему за абонентскую плату (абонентская плата может зависеть от набора клиентов и объема данных, проходящих в через сервис провайдера). Все управление приложениями, в том числе обновление, модернизация и техническая поддержка, обеспечивается провайдером.

Иногда к классической модели добавляют варианты, например DaaS (Data as a service – Данные как сервис/услуга, когда обеспечивается предоставление данных по требованию пользователя), Caas (Communication as a service – Коммуникации как сервис/услуга, когда предоставляются услуги связи, чаще всего IP-телефония) и т.д.

Существует несколько вариантов использования облачных систем: публичное облако, приватное облако, общее облако и гибридное облако, которые отличаются прежде всего тем, кому принадлежат используемые технологии и инфраструктура – пользователю или провайдеру [5]:

1. *Публичное облако* – доступ к технологиям имеет любой пользователь через сетевые каналы передачи данных (обычно Интернет), инфраструктура принадлежит организации, которая это облако создала. Именно в этом варианте вопросы обеспечения безопасности практически полностью возлагаются на провайдера.
2. *Приватные облака* – облака, создаваемые в основном для нужд конкретной организации. Инфраструктура может быть собственностью компании или арендоваться у провайдера, управление может осуществляться как самой организацией, так и провайдером, который обеспечивает ее обслужи-

вание. Этот подход позволяет организации максимально контролировать всю технологию работы с данными и обеспечить максимальную безопасность (естественно, при разработке и соблюдении соответствующей политики безопасности).

3. *Общее облако* – инфраструктура принадлежит нескольким организациям, которые объединились для достижения какой-либо цели. Инфраструктура может управляться самими организациями или выделенным сервис-провайдером.
4. *Гибридное облако* – используется совокупность двух или более облаков с разными моделями внедрения, объединенные общей технологией или стандартом.

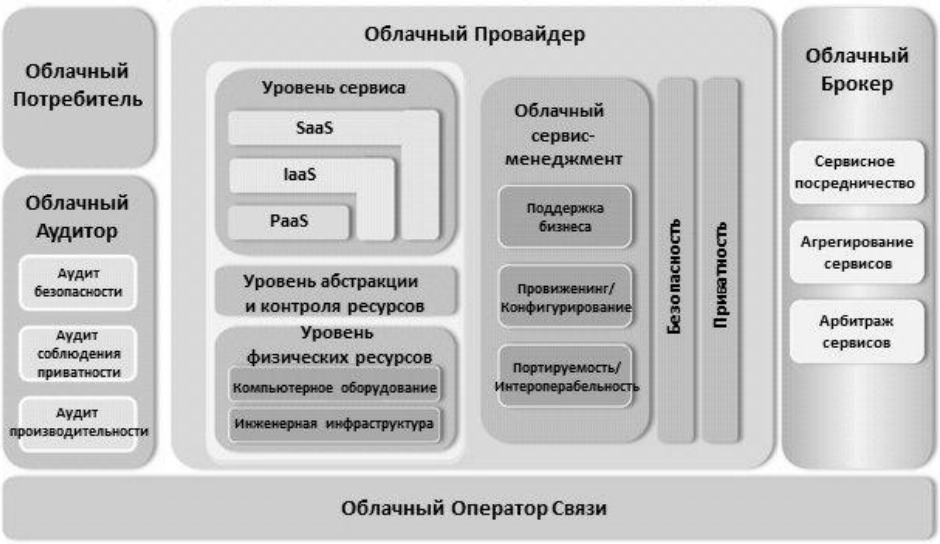

Рис. 1. Концептуальная диаграмма референтной архитектуры облачных вычислений

3. Проблемы обеспечения информационной безопасности в облачных сервисах. При перемещении данных и приложений в облака мы фактически уходим от понятия периметра, на котором строится вся защита классических систем: защищаться теперь должен не периметр, не инфраструктура обработки, хранения и передачи данных, принадлежность которой может быть неочевидной, а сама информация. Вопросы безопасности волнуют не только клиента – как провайдер будет обращаться с его данными, но и провайдера – насколько можно доверять клиенту, от каких внешних и внутренних угроз необходимо обеспечить защиту инфраструктуры. При этом основная доля рисков по защите данных ложится именно на провайдера – поставщика услуг.

Можно выделить следующие группы проблем информационной безопасности, возникающих при использовании облачных технологий, которые тормозят их внедрение:

1. Технологические и организационные проблемы:
   - ♦ необходимость изменения классических (изученных, отработанных и проверенных) подходов к обеспечению безопасности;
   - ♦ практически полное отсутствие соответствующих стандартов по безопасности (особенно в России);

- отсутствие методик оценки качества, оценки эффективности и оценки защищенности, сложность оценки рисков;
- недоработанные модели угроз и модели нарушителя;
- сложности в отслеживании причин нарушения безопасности;
- небезопасные программные интерфейсы (API);
- угроза завладения данными провайдером или его сотрудниками (инсайдерство) либо какой-либо третьей силой;
- отсутствие либо недостаток контроля над серверами и технологическими процессами;
- сомнения в корректности результатов облачных вычислений;
- специфические уязвимости, возникающие при использовании средств виртуализации в облаках: возможность несанкционированного взаимодействия между хостами и виртуальными машинами, проблемы с изоляцией хостов и виртуальных машин, различные виды атак, использующих, в частности, уязвимости гипервизоров;
- специфические требования к идентификации и аутентификации;
- дополнительные проблемы защиты подключений узлов организации к серверам провайдера-поставщика услуг.

2. Юридические проблемы:
   - отсутствие стандартов и законодательных актов;
   - размытая область ответственности из-за динамически изменяющейся инфраструктуры.
3. Антропогенные проблемы:
   - психологические сложности из-за необходимости передачи данных сторонним компаниям;
   - сложность оценки уровня доверия провайдеров;
   - недоверие и опаска по отношению к новым технологиям;
   - боязнь сокращений IT-персонала, что может привести к повышению риска инсайдерства.

4. Организации, занимающиеся проблемами безопасности облачных систем. Вопросами безопасности облачных систем занимается сразу несколько альянсов, наиболее авторитетным из которых считается Cloud Security Alliance (CSA), основанный в 2008 г. ведущими специалистами информационной безопасности предприятий, участвовавших в ассоциации Information Systems Security Association (ISSA), и ставящий своей целью распространение передового опыта по обеспечению безопасности при работе с облачными сервисами. В частности, этим альянсом был выпущен документ Security Guidance for Critical Areas of Focus in Cloud Computing – руководство по критически важным вопросам безопасного облачных вычислений.

В Европе аналогичные функции выполняет организация Jericho Forum, созданная в 2004 г. как площадка для обсуждения проблем защиты данных, возникающих в связи с уходом развитием модели без защищаемого периметра (депериметризации). Jericho Forum работает прежде всего с архитектурой, ориентированной на сотрудничество (Collaboration Oriented Architecture, COA). С появлением облачных вычислений Jericho Forum предложил руководящий документ Securely Collaborating in Clouds, в котором принципы COA распространены и на эту сферу [6].

Концепция облачных вычислений подвергалась активной критике, в частности, со стороны сообщества свободного программного обеспечения, например, со стороны Ричарда Столлмана: «Использовать веб-приложения для своих вычислительных процессов не следует, например, потому, что вы теряете над ними кон-

троль. И это не лучше, чем использовать любую проприетарную программу. Делайте свои вычисления на своём компьютере, используя программы, уважающие вашу свободу. Если вы используете любую проприетарную программу или чужой веб-сервер, вы становитесь беззащитными. Вы становитесь игрушкой в руках того, кто разработал это ПО» [7].

И эти опасения в целом оправданы, хотя инвестиции провайдеров облачных услуг в средства безопасности, как правило, гораздо выше, чем у непрофильных организаций, что в теории может привести к более высокому уровню защищенности. Но здесь мы опять возвращаемся к вопросу оценки уровня доверия к провайдеру. Не случайно говорят о появлении новых видов безопасности: репутационной (reputation) и прогностической (predictive) безопасности.

По словам Максима Эмма [5], директора департамента аудита компании Информзащита, с точки зрения оценки провайдера облачных вычислений в области обеспечения нформационной безопасности этим провайдером и западными компаниями рекомендовано придерживаться определенной методологии: аудит по стандарту SAS 70 Type II (этот стандарт не является специализированным для облачных вычислений, но он стал основным в отсутствие соответствующих регламентирующих актов). Желательны сертификация провайдера по ISO 27001 или следование практикам ISO 27002. К формальным способам оценки безопасности, которые могут применять российские компании, относится аттестация по требованиям ФСТЭК, наличие сертифицированных средств защиты, наличие лицензий ФСТЭК и ФСБ, наличие сертификата EIA/TIA-492 для ЦОД.

5. Требования к обеспечению безопасности для различных классов облачных систем. Были проанализированы существующие базовые методики анализа защищенности автоматизированных систем и сформулирован набор базовых требований к обеспечению безопасности облачных систем, краткий перечень которых приведен ниже:

1. Классификация и управление активами:
   - ♦ классификация информации. Основные принципы классификации;
   - ♦ маркировка и обработка информации.
2. Вопросы безопасности, связанные с персоналом:
   - ♦ включение вопросов информационной безопасности в должностные обязанности. Проверка персонала при найме и соответствующая политика;
   - ♦ соглашения о конфиденциальности. Условия трудового соглашения;
   - ♦ обучение и подготовка в области информационной безопасности;
   - ♦ реагирование на инциденты нарушения информационной безопасности и сбои. Информирование об инцидентах нарушения информационной безопасности. Информирование о сбоях ПО.
3. Физическая защита ЦОД:
   - ♦ охраняемые зоны. Периметр и контроль доступа в охраняемые зоны;
   - ♦ безопасность зданий, производственных помещений и оборудования;
   - ♦ выполнение работ в охраняемых зонах;
   - ♦ безопасность оборудования. Расположение и защита оборудования;
   - ♦ безопасность кабельной и электрической сети;
   - ♦ техническое обслуживание оборудования;
   - ♦ политика "чистого стола" и "чистого экрана";
   - ♦ вынос имущества, обеспечение безопасности оборудования, используемого вне помещений организации.
4. Управление передачей данных и операционной деятельностью:
   - ♦ операционные процедуры и обязанности, их оформление;

- процедуры в отношении инцидентов нарушения информационной безопасности;
- разграничение обязанностей;
- разграничение сред разработки и промышленной эксплуатации;
- управление средствами обработки информации сторонними лицами и/или организациями;
- планирование производительности, нагрузки и приемка систем;
- защита от вредоносного программного обеспечения. Мероприятия по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением;
- контроль изменений;
- резервирование информации;
- журналы действий оператора и регистрация ошибок;
- управление сетевыми ресурсами и средства контроля сетевых ресурсов;
- безопасность носителей информации;
- использование сменных носителей компьютерной информации;
- процедуры обработки информации;
- безопасность системной документации;
- соглашения по обмену информацией и программным обеспечением;
- системы публичного доступа;
- другие формы обмена информацией.

5. Контроль доступа:
   - требование бизнеса по обеспечению контроля в отношении логического доступа;
   - регистрация пользователей;
   - контроль в отношении паролей пользователей;
   - идентификация и аутентификация пользователя;
   - аутентификация пользователей в случае внешних соединений;
   - аутентификация узла;
   - автоматическая идентификация и процедуры регистрации с терминала;
   - политика в отношении логического доступа;
   - контроль в отношении локального и сетевого доступа пользователей;
   - управление привилегиями и правами доступа пользователей;
   - обязанности пользователей;
   - защита портов диагностики при удаленном доступе;
   - принцип разделения в сетях;
   - контроль сетевых соединений;
   - управление маршрутизацией сети;
   - безопасность использования сетевых служб;
   - контроль доступа к операционной системе;
   - контроль доступа к приложениям;
   - ограничение доступа к информации;
   - использование системных утилит;
   - периоды бездействия терминалов;
   - ограничения подсоединения по времени;
   - изоляция систем, обрабатывающих важную информацию.
6. Мониторинг доступа и использования системы:
   - мониторинг доступа и использования системы;
   - регистрация событий;

- синхронизация часов;
- работа с переносными устройствами и работа в дистанционном режиме;
- мероприятия по обеспечению информационной безопасности при проведении аудита систем;
- защита инструментальных средств аудита систем.

7. Разработка и обслуживание систем:
   - требования к безопасности систем;
   - анализ и спецификация требований безопасности;
   - безопасность в прикладных системах;
   - подтверждение корректности ввода данных;
   - подтверждение корректности данных вывода;
   - контроль обработки данных в системе;
   - меры защиты информации, связанные с использованием криптографии;
   - политика в отношении использования криптографии;
   - шифрование;
   - цифровые подписи и аутентификация сообщений;
   - сервисы неоспоримости;
   - управление ключами;
   - безопасность системных файлов;
   - безопасность в процессах разработки и поддержки;
   - технический анализ изменений в операционных системах;
   - процедуры контроля изменений;
   - контроль программного обеспечения, находящегося в промышленной эксплуатации;
   - контроль доступа к библиотекам исходных текстов программ;
   - ограничения на внесение изменений в пакеты программ;
   - скрытые каналы утечки данных и "троянские" программы;
   - разработка программного обеспечения с привлечением сторонних организаций.
8. Меры по обеспечению непрерывной работы системы.
   - вопросы управления непрерывностью бизнеса;
   - непрерывность бизнеса и анализ последствий;
   - разработка и внедрение планов обеспечения непрерывности бизнеса;
   - структура планов обеспечения непрерывности бизнеса;
   - тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса.
9. Соответствие требованиям:
   - соответствие требованиям законодательства;
   - защита учетных записей организации;
   - защита данных и конфиденциальность персональной информации;
   - предотвращение нецелевого использования средств обработки информации;
   - регулирование использования средств криптографии;
   - пересмотр политики безопасности и техническое соответствие требованиям безопасности.

По каждому требованию в рамках разрабатываемой методики конкретизированы следующие вопросы:

- модель развертывания, для которой данный критерий критичен;
- цель применения рекомендаций;

- ♦ угрозы, которые могут быть ликвидированы при применении данных рекомендаций.

Уже сейчас можно сказать, что спорить о том, работать с облачными технологиями или нет, уже поздно. Облака прочно вошли в нашу жизнь, и сейчас от разработки и исследования систем безопасности облачных технологий во многом будет зависеть будущее как самих сервисов, так и компаний, их использующих.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Батлер Б.* Насколько широко используются облачные технологии? Зависит от того, как спрашивают [Электронный ресурс] // Открытые системы [сайт]. URL: http://www.osp.ru/news/articles/2013/18/13035508/ (дата обращения: 20.10.2013).
2. ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing Internet Computing, September/October 2008 (vol. 12 no. 5), pp. 96-99 Carl Hewitt, Massachusetts Institute of Technology. URL: http://www.computer.org/csdl/mags/ic/2008/05/mic2008050096-abs.html (дата обращения: 20.10.2013).
3. NIST Cloud Computing Program [Электронный ресурс] // National Institute of Standards and Technology [сайт]. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (дата обращения: 20.10.2013).
4. NIST Референтная (эталонная) архитектура облачных вычислений (Cloud Computing Reference Architecture) Версия 1.0. [Электронный ресурс] // О Cloud Computing на русском [сайт]. URL: http://cloud.sorlik.ru/reference_architecture.html (дата обращения: 20.10.2013).
5. *Эмм М.* Облачные вычисления. Плюсы и минусы с точки зрения безопасности [Электронный ресурс] // Информационная безопасность в СПбГЭУ [сайт]. URL: http://pycode.ru/2011/02/cloud-computing/ (дата обращения: 20.10.2013).
6. *Черняк Л.* Безопасность: облако или болото? [Электронный ресурс] // Открытые системы [сайт]. URL: http://www.osp.ru/os/2010/01/13000673/ (дата обращения: 20.10.2013).
7. *Stallman R.* Cloud computing is a trap, warns GNU founder Richard Stallman», интервью газете The Guardian. 2008/09/29 URL: http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman (дата обращения: 20.10.2013).

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Пескова Ольга Юрьевна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: poy@tgn.sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел./факс: +78634371905; кафедра безопасности информационных технологий; к.т.н.; доцент.

Степовая Ксения Евгеньевна – e-mail: stepxen@yandex.ru; кафедра безопасности информационных технологий; студентка.

Peskova Olga Yur'evna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: poy@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone/fax: +78634371905; the department of security in data processing technologies; cand. of eng. sc.; associate professor.

Stepovaya Xenia Evgen'evna – e-mail: stepxen@yandex.ru; the department of security in data processing technologies; student.