Защита информации и администрирование в локальных сетях.

Содержание работы

**1.Защита информации**

1.1.Введение  
1.2.Пути и методы защиты информации в системах обработки информации  
1.2.1.Пути несанкционированного доступа  
1.2.2.Классификация способов и средств защиты информации  
1.3.Анализ методов защиты информации в системах обработки данных  
1.4.Особенности защиты информации в ПЭВМ

**2. Администрирование сети**  
2.1. Что такое администрирование сети?  
2.2. Каковы обязанности администратора сети?  
2.3. Какие существуют способы управления доступом к ресурсам, какова особенность управления доступом?  
2.4. Каковы основные принципы обеспечения сетевой безопасности?

**3. Литература.**

**1.Защита информации**

**1.Введение**

**Информационная безопасность**– это состояние защищённости информационной среды.

**Защита информации**представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

* конфиденциальность (confidentiality) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
* целостность (integrity) – избежание несанкционированной модификации информации;
* доступность (availability) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

* неотказуемость или апеллируемость (non-repudiation) – невозможность отказа от авторства;
* подотчётность (accountability) – обеспечение идентификации субъекта доступа и регистрации его действий;
* достоверность (reliability ) – свойство соответствия предусмотренному поведению или результату;
* аутентичность или подлинность (authenticity ) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Проблемы защиты информации в системах электронной обработки  данных (СОД) постоянно находятся  в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под системами электронной обработки  данных понимаются системы любой  архитектуры и любого функционального  назначения, в которых для обработки  информации используются средства электронно-вычислительной техники, а под защитой информации - использование специальных средств, методов и мероприятий с целью  предотвращения утери информации, находящейся  в СОД. Широкое распространение  и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и  обрабатываемой с СОД информации.

Четко обозначилось три аспекта уязвимости информации:

1. Подверженность физическому уничтожению или искажению.
2. Возможность несанкционированной (случайной или злоумышленной) модификации.
3. Опасность несанкционированного получения информации лицами, для которых она не предназначена.

Рассматривая в целом  проблемы ЗИ в ЭВМ можно выделить три основных, относительно самостоятельных, но не исключающих, а дополняющих  друг друга направления:

* совершенствование организационных и организационно-технических мероприятий технологии обработки информации в ЭВМ;
* блокирование несанкционированного доступа к обрабатываемой в ЭВМ информации;
* блокирование несанкционированного получения информации с помощью технических средств.

Основными факторами затрудняющими  решение проблемы защиты информации в ЭВМ являются:

* массовость применения;
* постоянно растущая сложность функционирования;
* разнообразие программного обеспечения персональных компьютеров, архитектурных решений и легкая адаптируемость для решения разнообразных задач пользователей.

Основные трудности в  реализации систем защиты состоят в  том, что они должны удовлетворять  двум группам противоречивых требований:

1. Исключение случайной или преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам и ресурсам системы всех пользователей.
2. Система защиты не должна создавать заметных неудобств пользователям в процессе из работы с использованием ресурсов СОД. В частности должны обеспечиваться:

* полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий;
* удобство работы с информацией для групп взаимосвязанных пользователей;
* возможности пользователям допускать своей информации.

Чтобы надежно защитить информацию, система защиты должна регулярно  обеспечивать защиту:

1. Системы обработки данных от посторонних лиц.
2. Системы обработки данных от пользователей.
3. Пользователей друг от друга.
4. Каждого пользователя от себя самого.

## 2.Пути и методы защиты информации в системах обработки информации

## Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования, а также риску хищения. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств и программного обеспечения.

## 1. Пути несанкционированного доступа

Несанкционированный доступ к информации, находящейся в ЛВС бывает:

* косвенным - без физического доступа к элементам ЛВС;
* прямым - с физическим доступом к элементам ЛВС.

В настоящее время существуют следующие пути несанкционированного получения информации (каналы утечки информации):

* применение подслушивающих устройств;
* дистанционное фотографирование;
* перехват электромагнитных излучений;
* хищение носителей информации и производственных отходов;
* считывание данных в массивах других пользователей;
* копирование носителей информации;
* несанкционированное использование терминалов;
* маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
* использование программных ловушек;
* получение защищаемых данных с помощью серии разрешенных запросов;
* использование недостатков языков программирования и операционных систем;
* преднамеренное включение в библиотеки программ специальных блоков типа “троянских коней”;
* незаконное подключение к аппаратуре или линиям связи вычислительной системы;
* злоумышленный вывод из строя механизмов защиты.

## 2.Классификация способов и средств защиты информации

Для решения проблемы защиты информации основными средствами, используемыми  для создания механизмов защиты принято  считать:

1. Технические средства - реализуются в виде электрических, электромеханических, электронных устройств. Вся совокупность технических средств принято делить на:

* аппаратные - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой СОД по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);
* физические - реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах).

1. Программные средства - программы, специально предназначенные для выполнения функций, связанных с защитой информации.

В ходе развития концепции  защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного  сохранения информации. Необходим комплексных  подход к использованию и развитию всех средств и способов защиты информации. В результате были созданы следующие  способы защиты информации (рис. 1):

     1. Препятствие - физически преграждает злоумышленнику путь к защищаемой информации (на территорию и в помещения с аппаратурой, носителям информации).

1. Управление доступом - способ защиты информации регулированием использования всех ресурсов системы (технических, программных средств, элементов данных).

Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому названному выше объекту персонального имени, кода , пароля и опознание субъекта или объекта про предъявленному им идентификатору;
* проверку полномочий, заключающуюся в проверке соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту;
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию обращений к защищаемым ресурсам;
* реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.
* Маскировка - способ защиты информации с СОД путем ее криптографического. При передаче информации по линиям связи большой протяженности криптографическое закрытие является единственным способом надежной ее защиты.
* Регламентация - заключается в разработке и реализации в процессе функционирования СОД комплексов мероприятий, создающих такие условия автоматизированной обработки и хранения в СОД защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Для эффективной защиты необходимо строго регламентировать структурное построение СОД (архитектура зданий, оборудование помещений, размещение аппаратуры), организацию и обеспечение работы всего персонала, занятого обработкой информации.
* Принуждение - пользователи и персонал СОД вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные способы защиты информации реализуются  применением различных средств  защиты, причем различают технические, программные, организационные законодательные  и морально-этические средства.

Организационными средствами защиты называются организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации СОД для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы СОД на всех этапах: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

К законодательным средствам защиты относятся законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

К морально-этическим средствам защиты относятся всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета, престижа человека или группы лиц.

## 3.Анализ методов защиты информации в системах обработки данных

Обеспечение надежной защиты информации предполагает:

1. Обеспечение безопасности информации в СОД это есть процесс непрерывный, заключающийся в систематическом контроле защищенности, выявлении узких и слабых мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.
2. Безопасность информации в СОД. Последняя может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.
3. Надлежащую подготовку пользователей и соблюдение ими всех правил защиты.
4. Что никакую систему защиты нельзя считать абсолютно надежной, надо исходить их того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

## 4.Особенности защиты информации в ПЭВМ

Особенностями ПЭВМ с точки зрения защиты информации являются:

      малые габариты и вес, что делает их легко переносимыми;

      наличие встроенного внутреннего запоминающего устройства большого объема, сохраняющего записанные данные после выключения питания;

      наличие сменного запоминающего устройства большого объема и малых габаритов;

      наличие устройств сопряжения с каналами связи;

      оснащенность программным обеспечением с широкими функциональными возможностями.

Основная цель защиты информации в ПЭВМ заключается в обеспечение ее физической целостности и предупреждении несанкционированного доступа к ней.

В самом общем виде данная цель достигается путем ограничения доступа посторонних лиц в помещения, где находятся ПЭВМ, а также хранением сменных запоминающих устройств и самих ПЭВМ с важной информацией в нерабочее время в опечатанном сейфе.

Наряду с этим для предупреждения несанкционированного доступа к информации используются следующие методы:

      опознавание (аутентификация) пользователей и используемых компонентов обработки информации;

      разграничение доступа к элементам защищаемой информации;

      регистрация всех обращений к защищаемой информации;

     криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);

криптографическое закрытие защищаемой информации в процессе ее непосредственной обработки.

Для **опознавания пользователей** к настоящему времени разработаны и нашли практическое применение следующие способы.

1. Распознавание по простому паролю. Каждому зарегистрированному пользователю выдается персональный пароль, который он вводит при каждом обращении к ПЭВМ.

2. Опознавание в диалоговом режиме. При обращении пользователя программа защиты предлагает ему назвать некоторые данные из имеющейся записи (пароль, дата рождения, имена и даты рождения родных и близких и т.п.), которые сравниваются с данными, хранящимися в файле. При этом для повышения надежности опознавания каждый раз запрашиваемые у пользователя данные могут быть разными.

3. Опознавание по индивидуальным особенностям и физиологическим характеристикам. Реализация данного способа предполагает наличие специальной аппаратуры для съема и ввода соответствующих параметров и программ их обработки и сравнения с эталоном.

4. Опознавание по радиокодовым устройствам. Каждому зарегистрированному пользователю выдается устройство, способное генерировать сигналы, имеющие индивидуальные характеристики. Параметры сигналов заносятся в запоминающие устройства механизмов защиты.

5. Опознавание по специальным идентификационным карточкам. Изготавливаются специальные карточки, на которые наносятся данные, персонифицирующие пользователя: персональный идентификационный номер, специальный шифр или код и т.п. Эти данные на карточку заносятся в зашифрованном виде, причем ключ шифрования может быть дополнительным идентифицирующим параметром, поскольку может быть известен только пользователю, вводиться им каждый раз при обращении к системе и уничтожаться сразу же после использования.

Каждый из перечисленных способов опознавания пользователей имеет свои достоинства и недостатки, связанные с простотой, надежностью, стоимостью и др.

**Разграничение доступа к элементам защищаемой информации** заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. Само разграничение может осуществляться несколькими способами.

1. По уровням секретности. Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, «секретно», «совершенно секретно», «особой важности» и т.п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней и запрещается доступ к массивам (базам) более высоких уровней.

2. Разграничение доступа по специальным спискам. Для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

3. Разграничение доступа по матрицам полномочий. Данный способ предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента.

4. Разграничение доступа по мандатам. Данный способ заключается в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

**Регистрация всех обращений к защищаемой информации**осуществляется с помощью устройств, которые контролируют использование защищаемой информации, выявляют попытки несанкционированного доступа к ней, накапливают статистические данные о функционировании системы защиты.

**Криптографическое закрытие защищаемой информации, хранимой на носителях** (**архивация данных**) заключается в использовании методов сжатия данных, которые при сохранении содержания информации уменьшают объем памяти, необходимой для ее хранения.

**Криптографическое закрытие защищаемой информации в процессе ее непосредственной обработки**осуществляется с помощью устройств программно-аппаратных комплексов, обеспечивающих шифрование и дешифрование файлов, групп файлов и разделов дисков, разграничение и контроль доступа к компьютеру, защиту информации, передаваемой по открытым каналам связи и сетям межмашинного обмена, электронную подпись документов, шифрование жестких и гибких дисков.

**2.Администрирование сети**

**1. Что такое администрирование сети?**

Управление ЛВС становится необходимым, когда у сетевого администратора возникает необходимость, а также возможность оперировать ее общим представлением. Обычно это касается сетей, имеющих сложную архитектуру. Администрирование компьютерных сетей подразумевает переход от управления работой отдельных устройство к анализу трафика на различных сетевых участках, управлению логической конфигурацией сети, ее рабочими параметрами. Таким образом, задачи администрирования можно разбить на две основные группы:

* контроль над функционированием сетевого оборудования;
* управление работой сети в целом.

**2.Каковы обязанности администратора сети?**

Ключевой целью администрирования ЛВС становится достижение и поддержание параметров работы информационной системы, наиболее точно соответствующих потребностям пользователя, который может оценить ее работу не по характеристикам трафика, используемым протоколам, скоростью отклика сервера на запросы и особенностям сценариев, а по работе программного обеспечения, постоянно запускаемого на его персональном компьютере.

Сетевой администратор - это специалист, в зону ответственности которого входит нормальная работа и рациональное использование ресурсов автоматизированной системы и вычислительных сетей. В администрирование информационных систем входит:

* установка и последующая настройка ЛВС;
* поддержание ее постоянной работоспособности;
* инсталляция основного ПО;
* ведение мониторинга сетей.

**3.Какие существуют способы и модели управления доступом к ресурсам, какова особенность управления доступом?**

Контроль доступа к  ресурсам лежит в основе обеспечения  сетевой безопасности, ограничивает доступ к конфиденциальной или чувствительной информации. Существует два основных способа управления доступом пользователя к ресурсам: на уровне ресурсов и на уровне пользователей.

Среди бесчисленного множества моделей можно выделить следующие, более-менее непересекающиеся и задающие базовую классификацию: MAC, DAC, RBAC и ABAC.

## MAC: Mandatory Access Control

(рус. мандатное управление доступом)

В основе модели лежат понятия «режима конфиденциальности» и «допуска». Режим конфиденциальности устанавливается для объектов (информации, систем, операций), в то время как допуск присваивается субъектам (гражданам или техническим средствам, которые пытаются получить доступ). Например, в простейшем случае сотрудник с уровнем допуска «для служебного пользования» получает доступ к объектам уровней «не секретно» и «для служебного пользования», но не получает доступа к объектам уровня «совершенно секретно».

Основное преимущество модели заключается в относительной простоте устройства, администрирования и использования. Основной недостаток – невысокая гибкость в широких и разноплановых инфраструктурах.

## DAC: Discretionary Access Control

(рус. дискреционное, или избирательное управление доступом)

Данная модель работает на основе списков управления доступом (ACL, access control lists), задающих однозначное соответствие между объектами, субъектами и возможными действиями (типами доступа, операциями).

Особенностью модели является необходимость наличия либо чётко выделенных владельцев ресурсов, управляющих доступом, либо суперадминистраторов, имеющих достаточно большие полномочия. В масштабных инфраструктурах применение модели затрудняется быстро возрастающей сложностью управления, проявляющейся в количестве и размере списков управления доступом.

## RBAC: Role-based Access Control

(рус. управление доступом на основе ролей)

Считается развитием избирательной модели. Отдельные права доступа к объектам группируются в роли, а уже роли назначаются субъектам. Сложность управления уменьшается за счёт уменьшения числа связей (а, следовательно, и размеров списков управления доступом), а также за счёт логического объединения схожих прав доступа. Следует отметить, что объединять в роли следует именно права доступа к объектам, а не группировать субъектов с помощью ролей.

Именно управление доступом на основе ролей является самым применяемым инструментом корпоративного управления доступом.

Одно из ключевых преимуществ модели – возможность реализации принципа разграничения полномочий (Segregation of Duties), более полно адресуя вопросы информационной безопасности.

Основной недостаток модели – необходимость предварительной и достаточно детальной разработки ролевых моделей, позволяющих затем предоставлять доступ через сопоставление субъектов и ролей.

## ABAC: Attribute­based Access Control

(рус. управление доступом на основе атрибутов)

Часто рассматривается как дополнение к модели управления на основе ролей, хотя изначально разрабатывалась как альтернатива ей. Вместо ролей данная модель оперирует понятием атрибутов, или свойств субъектов. В корпоративной среде такими атрибутами могут выступать подразделение сотрудника, его должность, способ подключения к корпоративной сети, время суток и так далее. Основываясь на заранее определённых правилах и политиках, доступ к объектам предоставляется при «правильных» значениях атрибутов субъекта.

Считается, что данная модель является наиболее современной, проще в применении и позволяет выстраивать очень гибкие системы управления доступом.

При управлении доступом на уровне ресурсов доступ к ресурсу  предоставляется тем, кто знает  необходимый пароль. Это самый  простой способ управления: для доступа  к ресурсу нужен пароль, который  известен тем, кому разрешен доступ. Недостаток этого метода — угроза «расползания»  паролей, которые, по случайности или  по небрежности\* могут стать известны посторонним.

**4. Каковы основные принципы обеспечения сетевой безопасности?**

1. **Простота использования информационной системы**. Данный принцип информационной безопасности заключается в том, что для минимизации ошибок следует обеспечить простоту использования информационной системы. Во время эксплуатации ИС пользователи и администраторы совершают непреднамеренные ошибки, некоторые из которых могут вести к невыполнению требований политик безопасности и снижению уровня информационной безопасности. Чем более сложны, запутанны и непонятны для пользователей и администраторов совершаемые ими операции, тем больше они делают ошибок. Простота использования ИС является необходимым условием для снижения числа ошибочных действий. При этом следует помнить, что данный принцип информационной [безопасности](https://arinteg.ru/articles/organizatsiya-sistemy-informatsionnoy-bezopasnosti-26382.html) не означает простоту архитектуры и снижение функциональности ИС.

2. **Контроль над всеми операциями**. Этот принцип подразумевает непрерывный контроль состояния информационной безопасности и всех событий, влияющих на ИБ. Необходим контроль доступа к любому объекту ИС с возможностью блокирования нежелательных действий и быстрого восстановления нормальных параметров [информационной](https://arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html) системы.

3. **Запрещено всё, что не разрешено**. Этот принцип ИБ заключается в том, что доступ к какому-либо объекту ИС должен предоставляться только при наличии соответствующего правила, отраженного, например, в регламенте бизнес-процесса или настройках защитного программного обеспечения. При этом основной функцией системы ИБ является разрешение, а не запрещение каких-либо действий. Данный принцип позволяет допускать только известные безопасные действия, а не заниматься распознаванием любой угрозы, что очень ресурсоёмко, невозможно в полной мере и не обеспечивает достаточный уровень ИБ.

4. **Открытая архитектура ИС**. Этот принцип [информационной](https://arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html) безопасности состоит в том, что безопасность не должна обеспечиваться через неясность. Попытки защитить информационную систему от компьютерных угроз путем усложнения, запутывания и скрытия слабых мест ИС, оказываются в конечном итоге несостоятельными и только отсрочивают успешную хакерскую, вирусную или инсайдерскую атаку.

5. **Разграничение доступа**. Данный принцип ИБ заключается в том, что каждому пользователю предоставляется доступ к информации и её носителям в соответствии с его полномочиями. При этом исключена возможность превышения полномочий. Каждой роли/должности/группе пользователей можно назначить свои права на выполнение действий (чтение/изменение/удаление) над определёнными объектами ИС.

6. **Минимальные привилегии**. Принцип минимальных привилегий состоит в выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ. Такие ограничения, тем не менее, не должны мешать выполнению работы.

7. **Достаточная стойкость**. Этот принцип информационной безопасности выражается в том, что потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач. Например, необходимо, чтобы взлом паролей доступа требовал от хакеров неадекватно больших промежутков времени и/или вычислительных мощностей.

8. **Минимум идентичных процедур**. Этот принцип информационной безопасности состоит в том, что в системе ИБ не должно быть общих для нескольких пользователей процедур, таких как ввод одного и того же пароля. В этом случае масштаб возможной хакерской атаки будет меньше.

**3.Литература**

https://studfile.net/preview/5996653/

https://www.yaneuch.ru/cat\_22/zashhita-informacii-i-administrirovanie-v/331285.2467907.page1.html

https://inform-ikt.narod.ru/book12.htm

https://alp-itsm.ru/interesting/administrirovanie\_kompyuternyh\_setej/#:~:text=%D0%90%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85%20%D1%81%D0%B5%D1%82%D0%B5%D0%B9%20%D0%BF%D0%BE%D0%B4%D1%80%D0%B0%D0%B7%D1%83%D0%BC%D0%B5%D0%B2%D0%B0%D0%B5%D1%82%20%D0%BF%D0%B5%D1%80%D0%B5%D1%85%D0%BE%D0%B4,%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B3%D1%83%D1%80%D0%B0%D1%86%D0%B8%D0%B5%D0%B9%20%D1%81%D0%B5%D1%82%D0%B8%2C%20%D0%B5%D0%B5%20%D1%80%D0%B0%D0%B1%D0%BE%D1%87%D0%B8%D0%BC%D0%B8%20%D0%BF%D0%B0%D1%80%D0%B0%D0%BC%D0%B5%D1%82%D1%80%D0%B0%D0%BC%D0%B8.

https://cleverics.ru/digital/2015/04/access-control-models/