Захарин Сергей Иванович, кандидат юридических наук., доцент кафедры Информационных технологий и математики

Лекция №.1
Информационная безопасность: понятия и определения

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

План лекции :

1.Основы информационной безопасности (И.Б.)

1.1.Понятие информационной безопасности

1.2.Основные составляющие информационной безопасности (И.Б.)

1.3.Важность и сложность проблемы информационной безопасности

2.Объектно-ориентированного подход – перспективный принцип анализа вопросов И.Б.

3.1. Необходимость применения объектно-ориентированного подхода к информационной безопасности

3.2. Основные понятия объектно-ориентированного подхода

3.3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

3.4. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Литература :

а) основная литература

1.Баранова Е. К. Моделирование системы защиты информации: Практикум: учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. - (Высшее образование: Бакалавр.). (znanium.com).

2.Партыка Т. Л. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. (znanium.com).

3.Бабаш А. В. Криптографические методы защиты информации. Том 3: учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. (znanium.com)

б) дополнительная литература

1.Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 2-е изд., стер. - М.: Академия, 2007. - 336 с.

2.Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. — 2006. — № 31. — Ст. 3448.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Понятие информационной безопасности

*Под **информационной безопасностью** будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.*

***Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.*

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1.Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться.

2.Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Отметим, что термин «компьютерная безопасность» (как эквивалент или заменитель понятия «информационная безопасность») представляется слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя в первую очередь внимание будет сосредоточено на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на листочке, прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Обратим внимание, что в определении ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

1.2 Основные составляющие информационной безопасности

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия **доступности, целостности и конфиденциальности.**

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент И.Б.

Целостность - можно подразделить на:

- **статическую,** понимаемую как неизменность информационных объектов;
- **динамическую,** относящуюся к корректному выполнению сложных действий.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность и наконец, конфиденциальные моменты есть также у многих организаций (например, пароли).

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

1.3 Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном. Для иллюстрации этого положения ограничимся несколькими нижеприведенными примерами из литературы.

В Доктрине информационной безопасности Российской Федерации (здесь, подчеркнем, термин «информационная безопасность» используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

-Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).

-Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

-Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском универси-

тете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

-В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом и т.д.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла ИС.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

2. ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Необходимость применения объектно-ориентированного подхода к информационной безопасности

В настоящее время информационная безопасность является относительно замкнутой дисциплиной, развитие которой не всегда синхронизировано с изменениями в других областях информационных технологий. В частности, в ИБ пока не нашли отражения основные положения объектно-ориентированного подхода, ставшего основой при построении современных информационных систем. Не учитываются в ИБ и достижения в технологии программирования, основанные на накоплении и многократном использовании программистских знаний. Это очень серьезная проблема, затрудняющая прогресс в области ИБ.

Попытки создания больших систем еще в 60-х годах вскрыли многочисленные проблемы программирования, главной из которых является сложность создаваемых и сопровождаемых систем. Результатами исследований в области технологии программирования стали сначала структурированное программирование, затем объектно-ориентированный подход.

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Представляется естественным и, более того, необходимым, стремление распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Любой разумный метод борьбы со сложностью опирается на принцип «divide et impera» - «разделяй и властвуй». Этот принцип означает, что сложная система (информационной безопасности) на верхнем уровне должна состоять из небольшого числа относительно независимых компонентов. Относительная независимость здесь и далее понимается как минимизация числа связей между компонентами.

Затем декомпозиции подвергаются выделенные на первом этапе компоненты, и так далее до заданного уровня детализации. В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции. Структурный подход опирается на алгоритмическую декомпозицию, когда выделяются функциональные элементы системы.

Основная проблема структурного подхода состоит в том, что он неприменим на ранних этапах анализа и моделирования предметной области, когда до алгоритмов и функций дело еще не дошло. Нужен подход «широкого спектра», не имеющий такого концептуального разрыва с анализируемыми системами и применимый на всех этапах разработки и реализации сложных систем. Мы постараемся показать, что объектно-ориентированный подход удовлетворяет таким требованиям.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

2. Основные понятия объектно-ориентированного подхода

Объектно-ориентированный подход использует объектную декомпозицию, то есть поведение системы описывается в терминах взаимодействия объектов.

Необходимо ввести понятие класса.

Класс - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Объект - это элемент класса, то есть абстракция определенной сущности.

Подчеркнем, что объекты активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми методами объекта. Например, может быть определен класс «пользователь», характеризующий «пользователя вообще», то есть ассоциированные с пользователями данные и их поведение (методы). После этого может быть создан объект «пользователь Иванов» с соответствующей конкретизацией данных и, возможно, методов.

Следующую группу важнейших понятий объектного подхода составляют:

- инкапсуляция,
- наследование,
- полиморфизм.

Основным инструментом борьбы со сложностью в объектно-ориентированном подходе является **инкапсуляция** - сокрытие реализации объектов (их внутренней структуры и деталей реализации методов) с предоставлением вовне только строго определенных интерфейсов.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Понятие «полиморфизм» может трактоваться как способность объекта принадлежать более чем одному классу. Введение этого понятия отражает необходимость смотреть на объекты под разными углами зрения, выделять при построении абстракций разные аспекты сущностей моделируемой предметной области, не нарушая при этом целостности объекта. (Строго говоря, существуют и другие виды полиморфизма, такие как перегрузка и параметрический полиморфизм, но нас они сейчас не интересуют.)

Наследование означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов. Наследование является важным инструментом борьбы с размножением сущностей без необходимости. Общая информация не дублируется, указывается только то, что меняется. При этом класс-потомок помнит о своих «предках».

Очень важно и то, что наследование и полиморфизм в совокупности наделяют объектно-ориентированную систему способностью к относительно безболезненной эволюции. Средства информационной безопасности приходится постоянно модифицировать и обновлять, и если нельзя сделать так, чтобы это было экономически выгодно, ИБ из инструмента защиты превращается в обузу.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Объекты реального мира обладают, как правило, несколькими относительно независимыми характеристиками. Применительно к объектной модели будем называть такие характеристики гранями.

Основными гранями ИБ является:

- доступностью,
- целостностью,
- конфиденциальностью.

Понятие грани позволяет более естественно, чем полиморфизм, смотреть на объекты с разных точек зрения и строить разноплановые абстракции.

Понятие уровня детализации важно не только для визуализации объектов, но и для систематического рассмотрения сложных систем, представленных в иерархическом виде. Само по себе оно очень простое: если очередной уровень иерархии рассматривается с уровнем детализации n>0, то следующий - с уровнем (n-1). Объект с уровнем детализации 0 считается атомарным.

Понятие уровня детализации показа позволяет рассматривать иерархии с потенциально бесконечной высотой, варьировать детализацию как объектов в целом, так и их граней.

Весьма распространенной конкретизацией объектно-ориентированного подхода являются компонентные объектные среды, к числу которых принадлежит, например, JavaBeans — классы в языке Java Весьма распространенной конкретизацией объектно-ориентированного подхода являются компонентные объектные среды, к числу которых принадлежит, например, JavaBeans — классы в языке Java, написанные по определённым правилам. Они используются для объединения нескольких объектов Весьма распространенной конкретизацией объектно-ориентированного подхода

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Здесь появляется два новых важных понятия: компонент и контейнер. Компонент можно определить как многократно используемый объект, допускающий обработку в графическом инструментальном окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество компонентов, образуя общий контекст взаимодействия с другими компонентами и с окружением. Контейнеры могут выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими объектно-ориентированному подходу:

- инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый вовне интерфейс;
- наследование позволяет развивать созданные ранее компоненты, не нарушая целостность объектной оболочки;
- полиморфизм по сути дает возможность группировать объекты, характеристики которых с некоторой точки зрения можно считать сходными.

Понятия же компонента и контейнера необходимы нам потому, что с их помощью можно естественным образом представить защищаемую ИС и сами защитные средства. В частности, контейнер может определять границы контролируемой зоны (задавать так называемый «периметр безопасности»).

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Применим объектно-ориентированный подход к вопросам информационной безопасности.

Проблема обеспечения информационной безопасности - комплексная, защищать приходится сложные системы, и сами защитные средства тоже сложны, поэтому нам понадобятся все введенные понятия. Начнем с понятия грани.

Фактически три грани уже были введены: это доступность, целостность и конфиденциальность. Их можно рассматривать относительно независимо, и считается, что если все они обеспечены, то обеспечена и ИБ в целом (то есть субъектам информационных отношений не будет нанесен неприемлемый ущерб).

Таким образом, мы структурировали нашу цель. Теперь нужно структурировать средства ее достижения. Введем следующие грани:

- законодательные меры обеспечения информационной безопасности;
- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

Отметим, что, в принципе, их можно рассматривать и как результат варьирования уровня детализации (по этой причине мы будем употреблять словосочетания «законодательный уровень», «процедурный уровень» и т.п.).

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия), административные меры - на всех субъектов в пределах организации, процедурные – на отдельных людей (или небольшие категории субъектов), программно-технические – на оборудование и программное обеспечение.

При такой трактовке в переходе с уровня на уровень можно усмотреть применение наследования (каждый следующий уровень не отменяет, а дополняет предыдущий), а также полиморфизма (субъекты выступают сразу в нескольких ипостасях - например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться).

Очевидно, для всех выделенных, относительно независимых граней действует принцип инкапсуляции (это и значит, что грани «относительно независимы»). Более того, эти две совокупности граней можно назвать ортогональными, поскольку для фиксированной грани в одной совокупности (например, доступности) грани в другой совокупности должны пробегать все множество возможных значений (нужно рассмотреть законодательные, административные, процедурные и программно-технические меры). Ортогональных совокупностей не должно быть много; думается, двух совокупностей с числом элементов, соответственно, 3 и 4 уже достаточно, так как они дают 12 комбинаций.

Продемонстрируем теперь, как можно рассматривать защищаемую ИС, варьируя уровень детализации.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Пусть интересы субъектов информационных отношений концентрируются вокруг ИС некой организации, располагающей двумя территориально разнесенными производственными площадками, на каждой из которых есть серверы, обслуживающие своих и внешних пользователей, а также пользователи, нуждающиеся во внутренних и внешних сервисах. Одна из площадок оборудована внешним подключением (то есть имеет выход в Internet).

При взгляде с нулевым уровнем детализации мы увидим лишь то, что у организации есть информационная система (см. рис. 2).

Рис. 2 - ИС при рассмотрении с уровнем детализации 0.

Уже здесь необходимо учесть законы, применимые к организациям, располагающим информационными системами. Возможно, какую-либо информацию нельзя хранить и обрабатывать на компьютерах, если ИС не была аттестована на соответствие определенным требованиям. На административном уровне могут быть декларированы цели, ради которых создавалась ИС, общие правила закупок, внедрения новых компонентов, эксплуатации и т.п. На процедурном уровне нужно определить требования к физической безопасности ИС и пути их выполнения, правила противопожарной безопасности и т.п. На программно-техническом уровне могут быть определены предпочтительные аппаратно-программные платформы и т.п.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

По каким критериям проводить декомпозицию ИС – в значительной степени дело вкуса. Будем считать, что на первом уровне детализации делаются видимыми сервисы и пользователи, точнее, разделение на клиентскую и серверную часть (рис. 3).

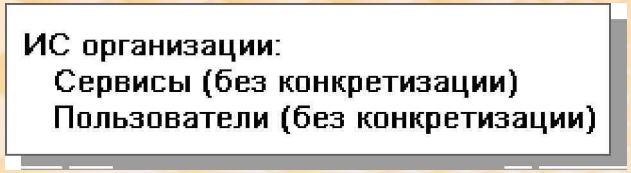

Рис. 3 - ИС при рассмотрении с уровнем детализации 1.

На этом уровне следует сформулировать требования к сервисам (к самому их наличию, к доступности, целостности и конфиденциальности предоставляемых информационных услуг), изложить способы выполнения этих требований, определить общие правила поведения пользователей, необходимый уровень их предварительной подготовки, методы контроля их поведения, порядок поощрения и наказания и т.п. Могут быть сформулированы требования и предпочтения по отношению к серверным и клиентским платформам.

На втором уровне детализации мы увидим следующее (см. рис. 4).

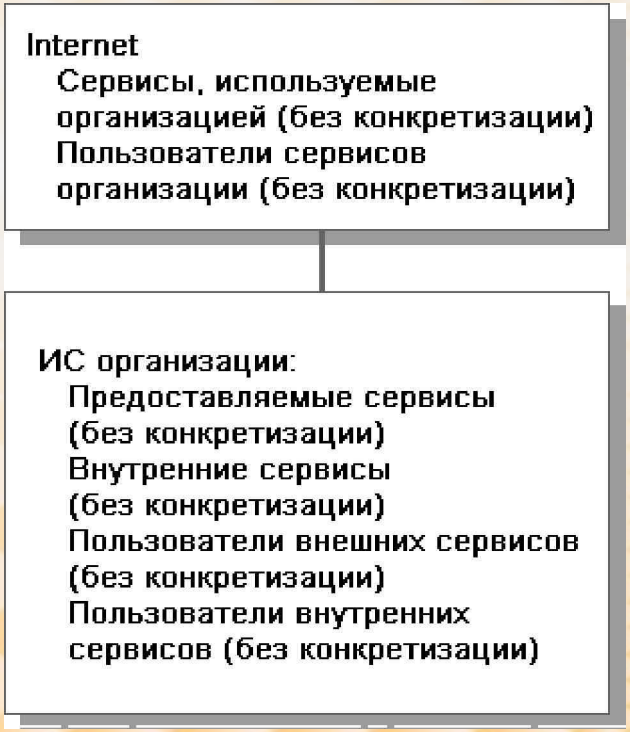

Рис. 4 - ИС при рассмотрении с уровнем детализации 2.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

На этом уровне нас все еще не интересует внутренняя структура ИС организации, равно как и детали Internet. Констатируется только существование связи между этими сетями, наличие в них пользователей, а также предоставляемых и внутренних сервисов. Что это за сервисы, пока неважно.

Находясь на уровне детализации 2, мы должны учитывать законы, применимые к организациям, ИС которых снабжены внешними подключениями. Речь идет о допустимости такого подключения, о его защите, об ответственности пользователей, обращающихся к внешним сервисам, и об ответственности организаций, открывающих свои сервисы для внешнего доступа. Конкретизация аналогичной направленности, с учетом наличия внешнего подключения, должна быть выполнена на административном, процедурном и программно-техническом уровнях.

Обратим внимание на то, что контейнер (в смысле компонентной объектной среды) «ИС организации» задает границы контролируемой зоны,

в пределах которых организация проводит определенную политику. Internet живет по другим правилам, которые организация должна принимать, как данность.

Увеличивая уровень детализации, можно разглядеть две разнесенные производственные площадки и каналы связи между ними, распределение сервисов и пользователей по этим площадкам и средства обеспечения безопасности внутренних коммуникаций, специфику отдельных сервисов, разные категории пользователей и т.п. Мы, однако, на этом остановимся.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Исходя из основных положений объектно-ориентированного подхода, следует в первую очередь признать устаревшим традиционное деление на активные и пассивные сущности (субъекты и объекты в привычной для дообъектной ИБ терминологии).

Подобное деление устарело, по крайней мере, по двум причинам.

Во-первых, в объектном подходе пассивных объектов нет. Можно считать, что все объекты активны одновременно и при необходимости вызывают методы друг друга. Как реализованы эти методы (и, в частности, как организован доступ к переменным и их значениям) - внутреннее дело вызываемого объекта; детали реализации скрыты, инкапсулированы. Вызывающему объекту доступен только предоставляемый интерфейс.

Во-вторых, нельзя сказать, что какие-то программы (методы) выполняются от имени пользователя. Реализации объектов сложны, так что последние нельзя рассматривать всего лишь как инструменты выполнения воли пользователей. Скорее можно считать, что пользователь прямо или (как правило) косвенно, на свой страх и риск, «просит» некоторый объект об определенной информационной услуге. Когда активизируется вызываемый метод, объект действует скорее от имени (во всяком случае, по воле) своего создателя, чем от имени вызвавшего его пользователя. Можно считать, что объекты обладают достаточной «свободой воли», чтобы выполнять действия, о которых пользователь не только не просил, но даже не догадывается об их возможности. Особенно это справедливо в сетевой среде и для программного обеспечения (ПО), полученного через Internet, но может оказаться верным и для коммерческого ПО, закупленного по всем правилам у солидной фирмы.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Для иллюстрации приведем следующий гипотетический пример. Банк, ИС которого имеет соединение с Internet, приобрел за рубежом автоматизированную банковскую систему (АБС). Только спустя некоторое время в банке решили, что внешнее соединение нуждается в защите, и установили межсетевой экран. Изучение регистрационной информации экрана показало, что время от времени за рубеж отправляются IP-пакеты, содержащие какие-то непонятные данные (наверное, зашифрованные, решили в банке).

Стали разбираться, куда же пакеты направляются, и оказалось, что идут они в фирму, разработавшую АБС. Возникло подозрение, что в АБС встроена закладка, чтобы получать информацию о деятельности банка. Связались с фирмой; там очень удивились, поначалу все отрицали, но в конце концов выяснили, что один из программистов не убрал из поставленного в банк варианта отладочную выдачу, которая была организована через сеть (как передача IP-пакетов специфического вида, с явно заданным IP-адресом рабочего места этого программиста). Таким образом, никакого злого умысла не было, однако некоторое время информация о платежах свободно гуляла по сетям.

Отметим, что при определении допустимости доступа важно не только (и не столько), кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя определить так называемые «троянские программы», выполняющие, помимо декларированных, некоторые скрытые (обычно негативные) действия.

Следует также признать устаревшим и положение о том, что разграничение доступа направлено на защиту от злоумышленников.

Приведенный выше пример показывает, что внутренние ошибки распределенных ИС представляют не меньшую опасность, а гарантировать их отсутствие в сложных системах современная технология программирования не позволяет.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

В дообъектной ИБ одним из важнейших требований является **безопасность повторного использования** пассивных сущностей (таких, например, как динамически выделяемые области памяти). Очевидно, подобное требование вступает в конфликт с таким фундаментальным принципом, как инкапсуляция. Объект нельзя очистить внешним образом (заполнить нулями или случайной последовательностью бит), если только он сам не предоставляет соответствующий метод. При наличии такого метода надежность очистки зависит от корректности его реализации и вызова.

Одним из самых прочных стереотипов среди специалистов по ИБ является трактовка операционной системы как доминирующего средства безопасности. На разработку защищенных ОС выделяются значительные средства, зачастую в ущерб остальным направлениям защиты и, следовательно, в ущерб реальной безопасности. В современных ИС, выстроенных в многоуровневой архитектуре клиент/сервер, ОС не контролирует объекты, с которыми работают пользователи, равно как и действия самих пользователей, которые регистрируются и учитываются прикладными средствами. Основной функцией безопасности ОС становится защита возможностей, предоставляемых привилегированным пользователям, от атак обычных пользователей.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Вопросы лекции:

1. Понятие информационной безопасности
2. Защита информации
3. Угрозы информационной безопасности
4. Основные составляющие информационной безопасности
5. Доступность
6. Целостность
7. Конфиденциальность
8. Целостность
9. Важность и сложность проблемы информационной безопасности
10. Необходимость применения объектно-ориентированного подхода к информационной безопасности
11. Класс
12. Объект
13. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

Презентация лекции

Информационная безопасность: понятия и определения

Захарин Сергей Иванович

Компьютерный набор, составление, техническое редактирование и озвучивание Захарин С.И.

Объем 2,0 п.л.

Захарин Сергей Иванович, кандидат юридических наук.,
доцент кафедры Информационных технологий и математики

КОНЕЦ ЛЕКЦИИ