**СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**MODERN PROBLEMS OF INFORMATION SECURITY**

Виноградова В.Г.

Санкт-Петербургский государственный экономический университет,

г. Санкт-Петербург, Россия

Исследованы теоретические и методические аспекты информационной безопасности. Проблема защиты информации с момента появления до современного состояния прошла длительный и во многом противоречивый путь в своем развитии, поэтому сейчас мы попробуем подробно и доступно рассмотреть данную актуальную проблему.

Ключевые слова: информационная безопасность, информационные системы, классификация, модель, информация.

Theoretical and methodological aspects of information security are investigated. The problem of information security from the moment of its appearance to the present state has passed a long and largely contradictory path in its development, so now we will try to consider this actual problem in detail and in an accessible way.

Keywords: information security, information systems, classification, model, information.

Изначально существовало два направления решения задачи поддержания конфиденциальности: использование криптографических методов защиты информации в средах передачи и хранения данных, и программно-техническое разграничение доступа к данным и ресурсам вычислительных систем. При этом стоит учесть, что в начале 80–х годов компьютерные системы были слабо распределенными, технологии глобальных и локальных вычислительных сетей находились на начальной стадии своего развития, и указанные задачи удавалось достаточно успешно решать. Позже, с появлением тенденции к распределенной обработке информации, классический подход к организации разделения ресурсов и классические криптографические протоколы начали постепенно исчерпывать себя и эволюционировать. Первостепенными стали проблемы аутентификации взаимодействующих элементов системы, а также способы управления криптографическими механизмами в распределенных компьютерных системах. Вместе с тем, начало складываться мнение о том, что функции криптографической защиты являются равноправными для автоматизированной системы и должны быть рассмотрены вместе с другими функциями. Данная теория послужила отправной точкой для разделения проблематики собственно средств защиты (включая криптографические средства, средства контроля доступа и др.) и средств обеспечения их корректной работы.

Так как процесс обеспечения информационной безопасности – это непрерывный процесс, то и существующая методология проектирования защищенной системы представляет собой итеративный процесс устранения найденных слабостей, некорректностей и неисправностей.

КЛАССИЧЕСКИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Угроза безопасности информации компьютерной системы (КС) – это потенциально возможное воздействие на информацию (КС), которое прямо или косвенно может нанести урон пользователям или владельцам информации (КС). Угрозы информационной безопасности могут быть разделены на два вида: естественные угрозы физических воздействий на информацию стихийных природных явлений – угрозы не зависящие от деятельности человека; искусственные угрозы –угрозы, вызванные человеческой деятельностью и являющиеся гораздо более опасными. Искусственные угрозы, в зависимости от их мотивов, разделяются на непреднамеренные (случайные) и преднамеренные (умышленные). К непреднамеренным угрозам относятся: ошибки в проектировании КС; ошибки в разработке программных средств КС; случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения; ошибки пользователей КС; воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др. Наибольшего внимания заслуживают искусственные преднамеренные угрозы, ввиду того, что вероятность этих угроз намного выше уже описанных.

К основным направлениям реализации злоумышленником информационных угроз относятся:

1)непосредственное обращение к объектам доступа;

2)создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

3)модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;

4)внедрение в технические средства системы программных или технических механизмов, нарушающих её предполагаемую структуру и функции.

При рассмотрении вопросов защиты автоматизированных систем целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой системе информации, которая поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т.е. поможет систематизировать и обобщить весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Эти уровни следующие:

1)уровень носителей информации; уровень средств взаимодействия с носителем;

2)уровень представления информации;

3)уровень содержания информации.

Данные уровни были введены исходя из того, что:

1)Информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть бумага, дискета или иной носитель;

2)Если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления.

Как уже было отмечено, информация может быть охарактеризована способом своего представления или тем, что еще называется языком в обиходном смысле.

КЛАССИФИКАЦИЯ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

1)методы и средства организационно-правовой защиты информации;

2)методы и средства инженерно-технической защиты информации;

3)криптографические методы и средства защиты информации;

4)программно-аппаратные методы и средства защиты информации.

ОРГАНИЗАЦИОННО–ПРАВОВЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ

К методам и средствам организационной защиты информации относятся организационно–технические и организационно–правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

Основные свойства методов и средств организационной защиты:

1)обеспечение полного или частичного перекрытия значительной части каналов утечки информации (например, хищения или копирования носителей информации);

2)объединение всех используемых в КС средств в целостный механизм защиты информации.

Методы и средства организационной защиты информации включают в себя:

1)ограничение физического доступа к объектам КС и реализация режимных мер;

2)ограничение возможности перехвата ПЭМИН;

3)разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок);

3)резервное копирование наиболее важных с точки зрения утраты массивов документов;

4)профилактику заражения компьютерными вирусами.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты, при этом далеко не все.

Можно выделить четыре уровня правового обеспечения информационной безопасности.

1)Международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России.

2)Подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ.

3)Государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.

4)Обеспечения информационной безопасности Локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

В руководящих документах Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ) приведены следующие основные способы несанкционированного доступа к информации в КС:

1)непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в него);

2)создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или преднамеренно оставленных разработчиком этих средств, так называемых «люков»);

3)модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);

4)внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

Модель нарушителя определяется исходя из следующих предположений:

1)нарушитель имеет доступ к работе со штатными средствами КС;

2)нарушитель является специалистом высшей квалификации (знает все о КС и, в частности, о системе и средствах ее защиты).

Можно выделить следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый следующий уровень включает в себя предыдущий):

1)Запуск программ из фиксированного набора (например, подготовка документов или получение почтовых сообщений);

2)Создание и запуск собственных программ (возможности опытного пользователя или пользователя с полномочиями отладки программ);

3)Управление функционированием КС – воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4)Весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включений в состав КС собственных СВТ с новыми функциями.

ЗАКЛЮЧЕНИЕ**:**Мы рассмотрели описание современные проблемы в области защиты информации с приведенной классификацией угроз безопасности компьютерных систем. Также была приведена классификация методов и средств защиты информации, описаны основные виды несанкционированного доступа к ресурсам автоматизированных систем. Показано, что основными способами защиты от несанкционированного доступа к информации в компьютерных системах являются аутентификация, авторизация (определение прав доступа субъекта к объекту с конфиденциальной информацией) и шифрование информации.

**Список используемой литературы:**

1)Жидких А.Д. Статья «Обучающая система».

2)Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Издательство Урал.университета, 2003. – 328 с.

3)Грушо А.А., Тимонина Е.Е. “Теоретические основы защиты информации” – Москва: Издательство Агентства “Яхтсмен”, 1996. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю.

4)Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192 с.