возможность кинематического анализа механизмов; имеется возможность эргономического анализа, как позы, так и движения, контроль поля зрения, зон досягаемости, усилий управления; продуманный и достаточно удобный интерфейс.

Таким образом, мы можем сказать, что в современном мире рынок программного обеспечения переполнен предложениями. Каждый может выбрать наиболее удобную для себя CAD систему, так как все они отличаются между собой как по функциональности, так и по стоимости.

1. Гулякин Д.В. Социально-информационная компетентность в структуре деятельности личности // Научные проблемы гуманитарных исследований. – 2009. – № 12. С. 36-39.
2. Гулякин Д. В. Роль информационно-коммуникационных технологий в формировании социально-информационной компетентности // Современные информационные технологии. – 2009. – №10. – с. 121-123.
3. Рагулин П.Г. Информационные технологии. Электронный учебник. - Владивосток: ТИДОТ Дальневост. ун-та, 2004. - 208 с.
4. Корнев В. В., Орлова Н. С., Улыбин А. В., Федотов С. Д., «Строительный контроль зданий и сооружений с применением мультипкоптеров и фотограмметрии».
5. BIM-технологии в строительстве: что это такое и зачем они нужны. [Электронный ресурс] – UPL <https://dmstr.ru/articles/bim/>

Самохвалова С.Г., Ложкова А.А.

Комплексная система защиты информации в организации

*ФГБОУ ВО «Амурский государственный университет»
(Россия, Благовещенск)*

doi: 10.18411/lj-05-2021-20

Аннотация

Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации.

Ключевые слова: Информационная безопасность, комплексная система защиты информации, аудит информационной безопасности, угрозы информационной безопасности, несанкционированный доступ, криптографическая защита.

Abstract

The problem of ensuring information security at all levels can be successfully solved only if a comprehensive information protection system is created and operates, covering the entire life cycle of computer systems from development to disposal and the entire technological chain of collecting, storing, processing and issuing information.

Keywords: Information security, integrated information security system, information security audit, information security threats, unauthorized access, cryptographic protection.

Защита информации подразумевает совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также доступности информации для пользователей. Защита информации – это целенаправленный, непрерывно продолжающийся процесс.

Комплексная система защиты информации в организации подразумевает ограничение доступа злоумышленников к базам данных, которые обрабатываются автоматизировано. Многие считают, что защита подразумевает только безопасность компьютерных сетей, но на самом деле термин «информация» включает широкий круг понятий из различных дисциплин.

Под информацией понимают:

- сведения и сообщения, различные осведомления о положении дел, которые передаются человеком различными способами;
- согласно математическому подходу – это различные сигналы, связанные с управлением, они имеют общие семантические, прагматические и синтаксические характеристики;
- по теории вероятности термин подразумевает неопределенность, которая уменьшается либо снимается при получении сообщения;
- отображение и передача разнообразий об объектах различной природы и процессах, связанных с ними.

Информация имеет большое значение для каждой организации. В защите нуждается информация двух типов:

- 1) Промышленная и научно-техническая информация
- 2) Коммерческая информация.

Понятие безопасности информации в организации

Под безопасностью информации подразумевается особое состояние, при котором невозможно ознакомление, воздействие, порча, кража и уничтожение данных сторонними лицами, которые не имеют прав на содержимое.

Параметры безопасности включают:

- доступность;
- целостность;
- конфиденциальность.

Комплексная система защиты должна обеспечить:

- защиту законных интересов организации от противоправных посягательств;
- охрану жизни и здоровья персонала;
- недопущение: 1) хищения финансовых и материально-технических средств; 2) уничтожения имущества и ценностей; 3) разглашения, утечки и несанкционированного доступа к служебной информации; 4) нарушения работы технических средств обеспечения производственной деятельности, включая информационные технологии.

Каналы несанкционированного доступа к данным

Доступ к информации посторонних может осуществляться через действующие в организации либо специально созданные каналы. Несанкционированный доступ может проводиться посредством вербовки сотрудников либо договора с ними, внедрения своих лиц в отделы, где сохраняется либо используется база данных организации. Доступ к конфиденциальной информации может быть реализован посредством физического проникновения к базам либо носителям, на которых хранятся данные.

Хищение происходит при подключении оборудования злоумышленника к каналам связи. Оно реализуется через прослушивание речи и телефонных переговоров, а также через подключения к средствам, хранящим, воспроизводящим либо отображающим конфиденциальную информацию, визуальная съемка ее.

Результат несанкционированного доступа может стать причиной банкротства и краха одного крупного подразделения либо организации в целом.

Виды угроз в локальной компьютерной сети

Угрозы безопасности информации в локальных сетях бывают случайными и преднамеренными.

Случайные потери происходят по вине пользователей в ситуациях, когда запускаются программы, способные безвозвратно удалить всю информацию на диске, например, режим форматирования носителя. Много информации теряется либо становится доступной вследствие воздействия вирусов, либо неосторожных действий

пользователей данной базы при воздействии на ключи, атрибуты базы и документов и опции по разграничению прав доступа.

Умышленные угрозы подразумевают несанкционированное активное воздействие с целью вывода из строя техники, порчи базы данных, а также дезорганизацию всей локальной сети. Данный тип угроз условно делят на два типа: пассивные и активные. Первая разновидность направлена на доступ, считывание, прослушивание информации скрытно без какого-либо воздействия на сам канал и хранимую информацию. Второй тип направлен на нарушения правильного функционирования отдельных звеньев либо всей цепи.

Методы комплексной защиты информации

Комплексная защита информации подразумевает предварительную разработку политики конфиденциальности с детальным описанием целей, но без конкретизации методов, которыми она будет достигнута.

Средства защиты условно можно разделить на формальные и неформальные. Первые подразумевают комплекс технических средств и программ, которые обеспечивают безопасность без вмешательства пользователя. Вторая разновидность – защита данных с привлечением человеческого фактора. Модель является визуальной реализацией целей политики и преобразует их термины информационных технологий. Она описывает структуру защиты, необходимые методы и средства, принципы авторизации в системе, обеспечение препятствий в качестве физической преграды к механизмам, звеньям и оборудованию.

Управление доступом подразумевает присвоение каждому потребителю информационного ресурса индивидуального идентификатора, например, посредством создания учетной записи с логином и паролем. Вход в систему возможен только при аутентификации в соответствии с выбранным типом идентификатора.

При работе с информационными ресурсами обязательно вводится регистрация запросов пользователя к этому ресурсу с обязательным протоколированием процесса.

При передаче данных по локальной сети и за ее пределы используется маскировка в виде создания зашифрованного канала с помощью сложных криптографических ключей, взломать которые достаточно сложно. Для этой цели пригодны любые алгоритмы шифрования с несколькими степенями защиты.

Обработка и хранение информации осуществляют по определенному регламенту с минимизацией возможности несанкционированного воздействия. Каждому процессу задаются определенные функции с правами доступа, исключающие искажение данных при совместной работе.

Защита локальных сетей от вирусов

На каждый компьютер локальной сети обязательно устанавливается антивирусное программное обеспечение, которое периодически проводит мониторинг состояния системы. Антивирус обновляется самостоятельно в фоновом режиме без участия пользователя. Существует несколько типов антивирусного программного обеспечения.

Программы-детекторы необходимы для обнаружения зараженных вирусом файлов. Они обнаруживают только широко известные вирусы, которые заложены в базу данных этой программы.

Программы-полифаги способны не только обнаружить зараженные файлы, но и уничтожить и «вылечить» их. Под лечением подразумевается удаление тела вируса из файла.

Программы-иммунизаторы представляют собой резидентные программы, не допускающие заражение файлов. Они уместны, когда на компьютерах не установлены антивирусы, уничтожающие зараженный файл.

Все вышеперечисленные компоненты входят в состав крупных антивирусных пакетов. Они включают программные библиотеки, по которым производится поиск

вредоносных компонентов. Вирусная база данных автоматически обновляется и пополняется. Именно из нее берется информация для сличения подозрительных объектов. Сканер и фильтр проверяют файлы на съемных носителях и во время типовых операций на компьютере.

Криптографическая защита

Под криптографией подразумевают способы преобразования информации для защиты от нежелательного использования либо воздействия.

Преобразование производится с помощью специальных алгоритмов шифрования. Шифрование может проводиться симметрично – создание только одного ключа, который шифрует и дешифрует данные, либо ассиметрично – создание двух ключей, один шифрует и является общедоступным, другой – дешифрует и является секретным.

Одним из способов шифрования является создание электронной цифровой подписи на основе ассиметричного алгоритма шифрования. Этот реквизит дает возможность проверить документ на наличие искажений с момента создания ключа, а также подтвердить принадлежность подписи владельцу сертификата этого ключа. Это специальный файл, который содержит в сжатом виде информацию о документе в виде зашифрованного образа.

Контроль целостности документов позволяет обнаружить подделку, в том числе при случайном воздействии на документ. Такая защита от изменений делает подделывание нерентабельным.

1. Грибунин, В. Г., Чудовский В.В., Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В.В. Чудовский. Москва : Издательский центр «Академия», 2009 г. – 416 с.
2. Блинов, А. М., Информационная безопасность : учеб. пособие. Часть 1 / А. М. Блинов. СПбГУЭФ, 2010 г. – 96 с.
3. Гатчин, Ю. А., Теория информационной безопасности и методология защиты информации : учеб. пособие / Ю. А. Гатчин, В. В. Сухостат. СПбГУ ИТМО, 2010 г. – 98 с.

Тимофеева Н.В., Костылев Н.С.

Проектирование системы информационной поддержки деятельности автошколы

*Северный (Арктический) федеральный университет имени М.В. Ломоносова
(Россия, Северодвинск)*

doi: 10.18411/lj-05-2021-21

Аннотация

Статья посвящена вопросу оптимизации деятельности автошколы с помощью внедрения системы информационной поддержки. В данной работе приведен вариант проектного решения проблем, возникающих в ходе поддержки учебного процесса.

Ключевые слова: автошкола, личное дело обучающегося, договор, теория, практика вождения, система информационной поддержки.

Abstract

The article is devoted to the issue of optimizing the activities of a driving school through the introduction of an information support system. In this paper, a variant of the design solution of problems arising in the course of supporting the educational process is given.

Keywords: driving school, student's personal file, contract, theory, driving practice, information support system.