ПОД-СЕКЦИЯ 3. Информатика, вычислительная техника и автоматизация

Михайлов Д.В.
к.т.н., доцент кафедры
Охраны труда и безопасности жизнедеятельности
Архитюк А.Ю.
студентка факультета
Инновационной экономики и кибернетики
Восточноукраинский национальный университет
имени Владимира Даля, г. Луганск

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сегодня общество все чаще и чаще задается вопросом об информационной безопасности. Внедрение информационных систем в повседневную жизнь каждого человека увеличивается с каждым днем. Сейчас уже мало кто представляет себе свою жизнь без компьютера, сети интернет, вне зависимости от возраста и вида деятельности. Во всех сферах жизни человека происходит автоматизация тех или иных процессов для удовлетворения постоянно возрастающих потребностей общества (автоматизация производства, торговли, оценки знаний, управления денежными средствами и т.д.). Ежедневно каждый член нашего общества сталкивается с проблемой конфиденциальности своей информации: ввод персональных данных на тех или иных ресурсах, использование электронных платежных систем, электронных ключей, банковских карт, ресурсов различного предназначения, и в каждом случае человек стремиться обезопасить себя и свои средства от постороннего вмешательства.

Информации может содержаться в любом элементе информационной системы (в файле, базе данных, программе, на сайте и т.д.). Эти объекты могут быть подвержены атакам асоциальных лиц, которые могут изменить, удалить, украсть, использовать в своих целях вашу информацию. Еще при создании какого-либо информационного объекта, его владелец устанавливает определенные критерии доступа к этому объекту, правила при работе с ним. Если умышленно нарушить эти правила, это будет квалифицироваться как атака на информацию. Информационная атака, по сути, определяется действиями злоумышленника, которые нарушают один или несколько свойств информации – конфиденциальность, доступность и целостность.

Свойство конфиденциальности отражается в разрешении или запрете на определенные права доступа к информации, информацию не сможет добыть неуполномоченное лицо, логический объект или процесс. Целостность информации позволяет сохранить информацию и не допустить ее изменения в результате несанкционированного доступа. Доступность подразумевает использование информации уполномоченным пользователем.

Перед проникновением в какую-либо информационную систему злоумышленники тщательно ее изучают, находят уязвимые места системы. Уязвимости можно найти и в организационно-правовом, и в программно-аппаратном обеспечении информационной системы.

Существует много моделей, связанных с защитой информации. Первой

опубликованной моделью была модель Биба, согласно которой все объекты и субъекты изначально делятся на несколько уровней доступа к информации, а потом накладываются ограничения на их взаимодействие, такие как: субъект не имеет возможности вызывать на исполнение субъекты с более низким уровнем доступа, субъекту запрещено модифицировать объекты с более высоким уровнем доступа. Модель Гогера-Гезингера базируется на теории автоматов. В соответствии с этой теорией система при каждом действии может переходить из одного допустимого состояния только в некоторые другие. Объекты и субъекты в этой модели защиты разделяются на группы – домены, а система может переходить из одного состояния в другое только согласно таблице разрешений, в ней указаны операции, которые может выполнять субъект. Переходы системы из одного состояния в другое происходит с помощью транзакции, это обеспечивает целостность системы.

Сазерландская модель защиты акцентирует внимание на взаимодействие потоков информации и субъектов. Есть машина состояний с множеством наборов начальных позиций и разрешенных комбинаций состояний. Модель Кларка-Вилсона занимает важное место в теории защиты информации. Она основана на оформлении определенных прав доступа субъектов к объекту и повсеместном применении транзакций. Впервые при исследованиях была затронута проблема третьей стороны, которая поддерживает всю систему безопасности. В информационных системах это чаще всего программа-супервизор. Транзакции в этой модели созданы по методу верификации, т.е. субъект идентифицировался перед выполнением первой команды от него и всех последующих. Считается, что данная модель максимально поддерживает целостность информационных систем.

Для безопасности информационной системы предприятия и для безопасности личных данных сотрудника необходимо постоянно проводить профилактические работы по разъяснению принципов информационной безопасности и правил, выполнение которых защитят информацию от злоумышленников. Основной акцент нужно делать на терминалы, работающие в публичных местах и офисах с более низким уровнем доступа к информации, однако, и при работе в помещениях с равным уровнем доступа не рекомендуется давать возможность сотрудникам работать за другими ЭВМ тем более в отсутствие владельца. В качестве программных профилактических мер используются экранные заставки с паролем, появляющиеся через 5-10 минут отсутствия рабочей активности, автоматическое отключение сервером клиента через такой же промежуток времени. Большое внимание следует уделять любым носителям информации, покидающим пределы фирмы. Необходимо помнить, что на рабочих поверхностях носителей даже в удаленных областях находится информация, которая может представлять либо непосредственный интерес, либо косвенно послужить причиной вторжения в систему.