профессионально и личностно значимых компетенций, наверное, дать невозможно. Это зависит от ряда факторов объективного и субъективного характера, среди которых можно назвать такие, как особенности образовательной программы, специфика дисциплины, личность преподавателя, психофизиологические особенности групп обучаемых и др.

Также необходимо помнить, что информационно-образовательная среда как в традиционном учебном процессе, так и в учебном процессе с применением дистанционных образовательных технологий никогда не сможет полностью заменить преподавателя и непосредственное общение с ним. Информационно-образовательная среда в общем случае содержит учебные материалы и регламентирующие учебный процесс документы, управляет же самостоятельной работой и самостоятельной познавательной деятельностью студентов преподаватель.

Библиографический список

1. Информационно-образовательная среда вуза [Текст]: учеб. пособие / *А.А. Карасик, Е.В. Чубаркова, А.О. Прокубовская, Т.В. Чернякова, Н.С. Власова, Н.В. Ломовцева, И.А. Суслова*. Екатеринбург: «Изд-во УНЦ УПИ», 2012. 80 с.

2. *Граф В., Ильясов И.И., Ляудис В.Я.* Основы организации учебной деятельности и самостоятельной работы студентов: учеб.-метод. пособие / В. Граф, И.И. Ильясов, В.Я. Ляудис В.Я. М.: Изд-во Моск.ун-та, 1981. 79 с.

Н.А. Руденков

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

nrudenkov@dlink.ru

Представительство «Д-Линк Интернешнл ПТЕ ЛТД», г.Екатеринбург

С развитием сетевых технологий персональный компьютер и обмен данными всё чаще заменяют людям «живое общение», а для определенной группы пользователей эти механизмы становятся, кроме того, орудием производства. И одной из основных задач для государственных, коммерческих служб и даже простых граждан становится вопрос об обеспечении безопасности информации.

Проблемы защиты информации привлекают всё большее внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей современных компьютерных средств, и, к сожалению – злоумышленников.

В широком смысле **информационная система –** есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией.

Информационная безопасность организации – состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

Иными словами, информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура – системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал.

Сетевая безопасность– это набор требований, предъявляемых к инфраструктуре компьютерной сети организации и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа.

Под сетевой безопасностью правильно понимать защиту информационной инфраструктуры объекта (организации) от вторжений злоумышленников извне, а также защиту от случайных ошибок персонала или намеренных действий инсайдеров внутри самой организации.

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.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение (персональные компьютеры и их составные части, а так же дисководы, принтеры, и т.д.);
- программное обеспечение (пользовательские программы, операционные системы и системные программы, утилиты, диагностические программы и т.д.);
- коммуникация (обеспечение передачи и обработки данных).

Типы угроз информационной безопасности

Исходя из определения понятия информационной безопасности, можно выделить три основных типа угроз:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения доступности системы (отказ в обслуживании).

Угрозы *нарушения конфиденциальности* направлены на разглашение конфиденциальной или секретной информации, то есть её компрометации. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Угрозы нарушения *целостности информации*, хранящейся в компьютерной системе или передаваемой посредством сети передачи данных, направлены на её изменение или искажение, приводящее к нарушению её качества или полному уничтожению. Целостность информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи).

Угрозы *нарушения доступности* системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые преднамеренные действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам.

Нарушение доступности системы может быть вызвано опасными воздействиями, которые условно, можно разделить на случайные и преднамеренные.

Причины *случайных воздействий* – аварийные ситуации из-за стихийных бедствий и отключения электроэнергии; отказы и сбои аппаратуры; ошибки в программном обеспечении; ошибки в работе обслуживающего персонала и пользователей; помехи в линии связи из-за

воздействия внешней среды, а также в следствии плотного трафика в системе (характерно для беспроводных решений и неуправляемых вычислительных сетей).

Преднамеренные воздействия связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, и т.д.

В общем случае, все угрозы информационной безопасности можно разделить на две группы: *внутренние и внешние*.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения внутренних угроз могут послужить: не здоровый климат в коллективе или низкая компетенция отдельных сотрудников с высоким уровнем самооценки, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет место так называемый «человеческий фактор», когда человек не умышленно, по ошибке, совершает действия, приводящие к нарушению информационной безопасности.

Внешние угрозы возникают благодаря непосредственной деятельности злоумышленников, из-за неумелой постановки взаимоотношений с представителями государственных структур, общественных организаций, средств массовой информации.

Действия извне могут быть направлены на:

- похищение или снятие копий с различных носителей информации;
- снятие информации в процессе коммуникации;
- снятие информации в процессе её передачи по сети связи;
- уничтожение информации или повреждение ее носителей;
- случайное или преднамеренное доведение до сведения конкурентов документов и материалов, содержащих конфиденциальную информацию.

Действия извне могут быть также направлены на персонал организации и выражаться в виде подкупа, угроз, шантажа, переманивания ведущих специалистов и т. п.

Система защиты информации

Наибольший эффект, в плане обеспечения информационной безопасности, достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – **систему защиты информации**.

Система защиты информации должна быть:

- Адекватной угрозам. Это предполагает тщательный анализ угроз как реальных, так и потенциальных и формирование требований к системе защиты информации конкретного объекта в конкретной обстановке.
- Непрерывной. Обеспечение информационной безопасности объекта – это непрерывный процесс, заключающийся в развитии системы зашиты, непрерывном контроле, выявлении её узких и слабых мест и потенциально возможных каналов утечки информации.
- Плановой. Разработка детального плана защиты информации каждого подразделения в сфере ее компетенции с учетом общей цели защиты.
- Централизованной. В рамках определенной структуры должна обеспечиваться организационно-функциональная самостоятельность процесса защиты информации.

- Целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд.
- Надежной. Методы и формы защиты должны надежно прерывать возможные каналы утечки информации, независимо от формы ее представления, языка выражения и вида физического носителя, на котором она закреплена.
- Универсальной. В зависимости от вида канала утечки его необходимо перекрывать, где бы он ни проявился, действенными и достаточными средствами, независимо от характера, формы и вида информации.
- Комплексной. Для защиты информации во всем многообразии структурных элементов и каналов утечки информации должны применяться все виды и формы в полном объеме.

Одной из важных мер организационного характера при формировании системы информационной безопасности, в первую очередь, следует считать разработку **политики информационной безопасности**. Политика информационной безопасности разрабатывается и реализуется высшим руководством организации (предприятия, учреждения и т.п.), и должна быть утверждена, документально издана и надлежащим образом доведена до всего персонала.

Организационно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия техническим средствам злоумышленников и формирования рубежей охраны объекта и оборудования с помощью комплексов технических средств, и включает в себя:

- сооружения(устройства) физической защиты от проникновения посторонних лиц на объект, а так же к линиям связи;
- средства защиты технических каналов утечки информации, возникающих при работе компьютерного оборудования, средств связи, и других приборов и офисного оборудования;
- средства защиты помещений от визуальных способов технической разведки;
- средства наблюдения (в т.ч. система видеонаблюдения), сигнализации, нарушений работы технических средств и изменений параметров сетей связи;
- средства обнаружения приборов и устройств технической разведки;
- технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов (флэш-накопители, магнитные носители информации и т.п.).

Рассматривая распределённую информационно вычислительную систему как структуру, состоящую из объектов разнесённых географически в пространстве и использующих для связи друг с другом публичные (открытые) сети, такие как Интернет, фактор обеспечения доступа к этим объектам имеет критическое значение, и является при этом важным аппаратно-программным элементом системы сетевой информационной безопасности.

Для обеспечения доступа к Интернет и надёжной защиты всей информационно вычислительной сети, в качестве устройства подключения учреждения следует применять т.н. межсетевые экраны. Межсетевые экраны – это специализированные аппаратные устройства, предлагающие всестороннюю защиту от несанкционированного доступа в сеть и нежелательного контента, а также от вирусных атак.

Серия устройств D-Link DFL NetDefend UTM оснащены системой обнаружения и предотвращения вторжения злоумышленниками, антивирусом и фильтрацией Web-

содержимого для проверки и защиты содержимого. Эти устройства позволяют распознавать угрозы и обеспечивать защиту сети, как против известных, так и против неизвестных сетевых атак.

По сути, устройства с таким функционалом по праву можно назвать средством коллективной информационной безопасности (СКИБ), и пренебрегать такими устройствами в информационно вычислительной сети учреждения было бы не разумно.

Литература:

1. Сайт компании D-Link. http://www.dlink.ru
2. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» ГОСТ Р ИСО/МЭК 17799–2005.
3. *Богданова Е.А., Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М.* «Технологии защиты в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы». «ИНТУИТ», 2013.–743с;

Ю.И. Самойленко

ОСОБЕННОСТИ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В ОБЛАСТИ ИЗУЧЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

yuroy@bk.ru
Международный университет природы, общества и человека «Дубна», Дубна

The article defines main principles and characteristics of the information and educational environment, describes its basic components and proposes to include web-based information and analytical services for implementation of the adaptive education process in the computer science field of study. The current state of this work in the «Dubna» University is described.

Теория и практика построения информационно-образовательных сред (ИОС) получили свое начало вследствие развития процесса информатизации образования. В специальной литературе на сегодняшний день существуют различные определения ИОС, в одних делается акцент на педагогическую составляющую, в других – на технические средства реализации. Невзирая на различия в формулировках, ИОС в первую очередь предназначена для повышения эффективности и доступности образовательного процесса подготовки специалистов, а также повышения качества обучения. В дальнейшем при изложении материала мы будем придерживаться формулировки ИОС как единого информационно-образовательного пространства, построенного с помощью интеграции информации на традиционных и электронных носителях, компьютерно-телекоммуникационных технологиях взаимодействия, включающего в себя виртуальные библиотеки, распределенные базы данных, учебно-методические комплексы и расширенный аппарат дидактики [1].

Учитывая общую концепцию построения ИОС, а также современное состояние разработок в данной области, состояние информационных технологий и других решений в области информатизации образования [2], можно определить принципы, на которых должны строиться современные ИОС.

Интегральность — ИОС должна включать в себя всю необходимую совокупность базовых знаний, определяемых профилями подготовки специалистов, содержать информационно-справочную базу дополнительных учебных материалов.