УДК 004.681

АНАЛИЗ УГРОЗ, ВОЗНИКАЮЩИХ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Волхонская Е.Е.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: lizaveta5.6@mail.ru*
Чупринина А.С.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: anna.chuprinina.02@mail.ru*
Падучих Д.В.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: dasha-oleinikova2002@mail.ru*

На сегодняшний день вопрос обеспечения информационной безопасности один из наиболее актуальных в сфере информационных технологий. Защита информации всегда была на ведущих ролях, поэтому особенно важно проводить объективную, независимую оценку текущего уровня защищенности информации. Изучены понятия, связанные с информационной безопасностью технически сложных объектов. Были рассмотрены угрозы, возникающие при обеспечении безопасности ТСО. Систематизирована информация о видах воздействия на информационную среду. Изучены виды средств защиты информации, определена принадлежность активных средств защиты к техническим средствам. Анализируются существующие подходы к анализу векторов угроз безопасности информации в АСУТП. Формулируется и обосновывается тезис о том, что большинство декларируемых угроз АСУТП относятся к автоматизированным системам в целом, а не только к АСУТП. Приводятся вектора угроз, существующих на полевом уровне АСУТП, которые в последующем могут лечь в основу разработки соответствующих методов и средств защиты. В данной статье будут рассмотрены основные понятия, связанные с базами данных, выявлены предъявляемые к ним требования, а также детально рассмотрены основные виды моделей данных, применяемые при проектировании баз данных.

Ключевые слова: автоматизированные системы, данные, информация, информационная безопасность.

ANALYSIS OF THREATS ARISING WHEN PROVIDING INFORMATION SECURITY OF AUTOMATED SYSTEMS

Volkhinskaya E.E.[1]
[1]*Samara State Technical University, Samara, e-mail: lizaveta5.6@mail.ru*
Chuprinina A.S.[1]
[1]*Samara State Technical University, Samara, e-mail: anna.chuprinina.02@mail.ru*
Paduchikh D.V.[1]
[1]*Samara State Technical University, Samara, e-mail: dasha-oleinikova2002@mail.ru*

To date, the issue of ensuring information security is one of the most relevant in the field of information technology. Information security has always been at the forefront, so it is especially important to conduct an objective, independent assessment of the current level of information security. The concepts related to the information security of technically complex objects are studied. The threats that arise when ensuring the safety of TSS were considered. Systematized information about the types of impact on the information environment. The types of means of information protection are studied, the belonging of active means of protection to technical means is determined. Existing approaches to the analysis of vectors of information security threats in process control systems are analyzed. The thesis is formulated and substantiated that most of the declared threats to APCS relate to automated systems in general, and not just to APCS. Vectors of threats that exist at the field level of the process control system are given, which can subsequently form the basis for the development of appropriate methods and means of protection. This article will discuss the basic concepts associated with databases, identify the requirements for them, and also consider in detail the main types of data models used in database design.

Keywords: emergency systems, data, information, information security.

Угрозы, возникающие при обеспечении информационной безопасности

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность [1].

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

1. должно стать известно о средствах использования пробела в защите;
2. должны быть выпущены соответствующие заплаты;
3. заплаты должны быть установлены в защищаемой ИС.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов. Они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Угрозы можно классифицировать по нескольким критериям:

1. по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
2. по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
3. по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
4. по расположению источника угроз (внутри/вне рассматриваемой ИС).[2]

Самыми частыми и самыми опасными являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами, иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Факторы, воздействующие на защищаемую информацию

Под факторами, воздействующими на защищаемую информацию, подразумевают явления, действия или процессы, результатом которых могут бытьутечка, искажение, уничтожение защищаемой информации или блокированиедоступа к ней.

Различают объективные и субъективные факторы и в каждом классе выделяют внешние и внутренние факторы.

Выявление факторов, воздействующих на защищаемую информацию,должно осуществляться с учетом следующих требований:

1. достаточности уровней классификации факторов, воздействующих незащищаемую информацию, позволяющих формировать их полное множество;

2. гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры классификации. В таблице 1 представлена классификация факторов, которые могут воздействовать на защищаемую информацию.[3]

Таблица 1 – факторы, воздействующие на защищаемую информацию

Факторы, воздействующие на защищаемую информацию		
Объективные	Внутренние	1. Передача сигналов по проводным и оптико-волоконным линиям связи 2. Излучения акустических, речевых и неречевых сигналов 3. Излучения в радио- и оптическом диапазонах 4. Побочное и паразитное электромагнитные излучения 5. Различные наводки 6. Дефекты, сбои, отказы, аварии ТС, систем и ПО
	Внешние	1. Явления техногенного характера. 2. Электромагнитные и радиационные облучения 3. Сбои, отказы и аварии систем обеспечения ОИ 4. Природные явления, стихийные бедствия 5. Термические (пожары и т.д.) 6. Климатические (наводнения и т.д.) 7. Механические (землетрясения и т.д.) 8. Электромагнитные (грозовые разряды и т.д.) 9. Биологические (микробы, грызуны и т.д.) 10. Химические факторы (химически агрессивные среды и т.д.)
Субъективные	Внутренние	1. Разглашение информации, опубликование в СМИ 2. Передача, утрата, хищение, копирование носителей информации 3. Несанкционированные доступ, изменение, копирование 4. Несанкционированное использование ПО («маскарад», 5. использование дефектов, применение вирусов) 6. Неправильная организация ЗИ (ошибки в задании требований, в организации контроля, несоблюдение требований) 7. Ошибки обслуживающего персонала (при эксплуатации 8. ТС/ПС/средств и систем ЗИ)
	Внешние	1. Доступ к защищаемой информации с применением технических средств разведки (радио- и оптико-электронной, 2. фото, визуальной, гидроакустической, компьютерной) и 3. съема информации 4. Несанкционированное подключение к ТС и системам 5. Использование ПО ТС ОИ («маскарад», использование 6. дефектов, применение вирусов) 7. Несанкционированный физический доступ на ОИ, хищение носителя 8. Блокирование доступа к защищаемой информации 9. Преступные действия и диверсии в отношении ОИ

Средства защиты информации

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации [4].

Средства обеспечения защиты информации в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.
2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).
3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.[5]

Технические средства защиты информации

Технические средства защиты – это механические, электромеханические, оптические, радио, радиолокационные, электронные и другие устройства и системы, способные выполнять самостоятельно или в комплексе с другими средствами функции защиты данных.

Технические средства защиты делятся на физические и аппаратные. К физическим средствам относятся замки, решетки, охранные сигнализации, оборудование КПП и др.; к

аппаратным – замки, блокировки и системы сигнализации о вскрытии, которые применяются на средствах вычислительной техники и передачи данных.

Средства защиты информации можно разделить на:

1. Средства, предназначенные для защиты информации. Эти средства не предназначены для непосредственной обработки, хранения, накопления и передачи защищаемой информации, но находящиеся в одном помещении с ними.Делятся на:

1.1. пассивные – физические (инженерные) средства, технические средства обнаружения, ОС, ПС, СКУД, ВН, приборы контроля радиоэфира, линий связи и т.п.;

1.2. активные – источники бесперебойного питания, шумогенераторы, скремблеры, устройства отключения линии связи, программно-аппаратные средства маскировки информации и др.;

2. Средства, предназначенные для непосредственной обработки, хранения, накопления и передачи защищаемой информации, изготовленные в защищенном исполнении. НИИЭВМ РБ разрабатывает и выпускает защищенные носимые, возимые и стационарные ПЭВМ;

Список литературы

1) Средства защиты информации (СЗИ) [Электронный ресурс]// Защита информации/ Департамент цифрового развития Смоленской области // URL: https://it-security.admin-smolensk.ru/zinfo/szi/

2) Пассивные и активные методы и способы защиты каналов утечки информации [Электронный ресурс]//studfile// URL:https://studfile.net/preview/5868802/

3) Активные методы защиты информации от утечки по электромагнитному и акустическому каналам [Электронный ресурс]//Helpiks// URL: https://helpiks.org/8-62604.html

4) Обеспечение сетевой безопасности совместно с брокерами сетевых пакетов. Часть вторая. Активные средства безопасности [Электронный ресурс]// Хабр// URL: https://habr.com/ru/company/dsol/blog/551124/

5) Пассивные и активные средства защиты информации[Электронный ресурс]// Техника для спецслужб // URL:http://www.bnti.ru/showart.asp?aid=547&lvl=04.03.