Бабичева Зульфия Викторовна

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Распределенные автоматизированные системы

Защита информации в распределенных информационных системах

Аннотация. Статья представляет собой развернутое положение в области исследования современных требований, которые предъявляются к определению уровня обеспечения информационной безопасности, и существенному росту рисков (финансовых, материальных, моральных, информационных) вследствие нарушения информационной безопасности во всех сферах жизнедеятельности государства и общества. Данные риски диктуют необходимость использования в деятельности предприятий эффективных средств и методов, позволяющих всесторонне оценить степень защищенности распределенных автоматизированных систем, а также обоснованности затрат на информационную безопасность, что и будет рассмотрено в данной статье.

Ключевые слова: информационная система, информационное обеспечение, база данных, информационная безопасность, система защиты информации.

Понятие информации в определении информационного обеспечения является первостепенным. В контексте обработки информации при изучении информационного обеспечения, немаловажное значение имеет понятие данных. Но существует различие между информацией и данными, которое заключается в конкретной форме представления, в данном случае данные являются определенным подмножеством предоставленной информации, которое определяется задачами и целями сбора и обработки информации.

Человеческий прогресс подарил великое множество достижений, но одновременно и породил массу проблем. Человечество, разрешая одни проблемы, одновременно сталкивается при этом и с другими, новыми проблемами, таким образом, защита информационных данных является актуальной проблемой всегда.

Проблема создания системы защиты информации (СЗИ) включает в себя две задачи, которые взаимно дополняют друг друга [4, с. 11]:

– разработка СЗИ, то есть ее синтез;

– оценка спланированной и созданной СЗИ.

Оценивание системы информационной защиты достигается анализом ее технических характеристик для того, чтобы установить, соответствует ли система защиты информации требованиям к данным системам.

Классификация методов и средств обеспечения информационной безопасности информации показана на рисунке [5, с. 36].

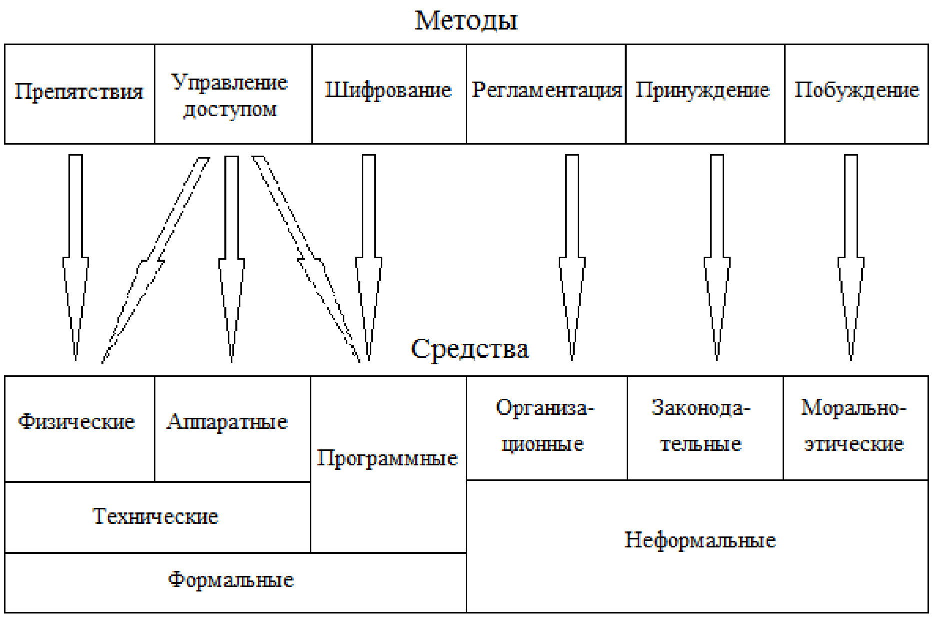

Рисунок. Методы и средства обеспечения безопасности информации

Одним из актуальных вопросов в области защиты информационной системы является разработка методологии в области создания и

совершенствования инструментального обеспечения контроля безопасности информации предприятия и структуры IT.

Обобщенная оценка эффективности системы защиты информации связана с определением взаимосвязи с целевым предназначением в определенных условиях функционирования.

В зависимости от сложности объема и систем, при решении задач, можно предположить, что провести оценку эффективности информационной системы в полной мере можно только при помощи системы показателей. Оценка эффективности достижения главных требований, которые в первую очередь соответствуют информационным системам, опирается на показатели оперативности, непрерывности, устойчивости, а также конфиденциальности.

В связи с этим, можно утверждать, что разработка методологии в области создания и совершенствования инструментального обеспечения контроля безопасности информации учреждений в целом является своевременной и актуальной. Информация по инцидентам, которые приводят к нарушению безопасности, требуется для анализа рисков и увеличения области применения результатов данного анализа. Такая информация должна быть собрана и обработана в общем объеме, поэтому необходимо, чтобы каждое предприятие обладало схемой анализа инцидентов (IAS, от англ. Incident analysis scheme) для поддержания процесса анализа рисков и управления другими аспектами деятельности организации, взаимосвязанными с безопасностью.

Необходимо отметить, что если некоторые предприятия находят выгодным использование процедуры обработки инцидентов, то другие считают, наиболее выгодным будет процесс объединения данной информации путем создания общей базы данных по инцидентам, что в свою очередь позволит гораздо быстрее получать предупреждения, идентифицировать тенденции и принимать меры защиты, в случае атаки. Общая база данных по инцидентам должна быть достаточно гибкой для того, чтобы учитывать требования общих (все секторы, типы угроз и их возможные воздействия) и частных (отдельные секторы, угрозы и их воздействия) интересов. Каждая

процедура обработки инцидентов, внутри или вне организации, должна использовать одинаковую типологию, метрологию и структуру программного обеспечения для регистрации информации по инцидентам. Это облегчает сравнение и анализ. Использование общей структуры является ключевым моментом для получения всеобъемлющих результатов и в особенности более достоверной базы данных для быстрой идентификации «предупреждения», которое невозможно получить от одиночной процедуры обработки инцидентов [1].

Можно сказать, что увеличение эффективности от использования процедуры обработки инцидентов будет способствовать взаимосвязи между процедурой обработки инцидентов, процессом анализа рисков, а также методами управления. Последствиями данных процессов будет являться, повышение качества выявления актуальных угроз, а, следовательно, качество оценки рисков, так как в данном случае создается и объединяется новая дополнительная информация об уязвимости информационных систем и способах их устранения.

Внедрение новой процедуры обработки инцидентов в будущем даст организации возможность идентификации и оценки уязвимости информационной системы, а также позволяет предоставить полезные входные данные с целью оценки вероятных рисков. Полученные данные с одной стороны базируются на информации об угрозах, а с другой на результатах расследования инцидентов, проводимых группой обеспечения компьютерной безопасности в случае аварийной ситуации. Поэтому внедрение процедуры обработки инцидентов в качестве идентификации и оценки уязвимостей поможет использовать информацию об угрозах, внедренную в базу данных о возможных инцидентах, вместе с информацией от других источников, особенно подразделениями служб компьютерной безопасности, которые могут обнаружить уязвимости, которые не были идентифицированные ранее [3, с. 45].

Также следует отметить, что внедряемая процедура обработки инцидентов касается инцидентов, которые уже произошли. Данная процедура

не дает непосредственного доступа к информации о присутствующих уязвимостях, и не проявленных. Помимо этого, данные по обработке инцидентов в статистическом анализе и анализе тенденций следует использовать с особой осторожностью, так как входные данные по результатам проведения работ могут быть либо ошибочными, либо неполными. Не смотря на это, результаты работы группы обеспечения компьютерной безопасности в аварийных ситуациях могут указать на наличие ранее незамеченных уязвимостей.

Последствиями воздействий компьютерных атак могут стать блокирование управляющей информации и внедрение дезинформации в командную информацию, нарушение установленных регламентов обработки информации в комплексах управления информационной системы, отказы и сбои в работе измерительных комплексов, а также компрометация информации.

В отличие от уязвимостей атака на информационную систему является активным элементом, то есть информационная система может и не иметь уязвимостей – тогда в соответствии с перечисленными выше методами атак, задачей нарушителя будет создать соответствующие условия для проведения атаки [4, с. 15].

Важным пояснением к разрабатываемому методу является то, что в распределенной информационной системы все подсистемы должны иметь одинаковую степень защищенности, так как угроза может быть реализована в результате атаки на любой из её элементов.

Также, при помощи предложенного метода можно осуществлять декомпозицию угроз и способов их реализации по заданным типам нарушителей, что в свою очередь позволит определить риски, которые создаются теми или иными потенциальными злоумышленниками, а также составить модель нарушителя исходя из их потенциальной опасности. При этом, моделирование таких рисков показывает, что наибольшую опасность представляют так называемые инсайдеры – сотрудники, наделенные соответствующими легальными полномочиями. Им гораздо проще получить

доступ к интересующей их информации, чем любому постороннему лицу. Да и практика расследований также свидетельствует о том, что успешность атаки напрямую зависит от наличия в организации сотрудника, который способствует её реализации.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016) Электронный ресурс] // Режим доступа: www.consultant.ru

2. Варфоломеева А.О., Коряковский А.В., Романов В.П. Информационные системы предприятия: Учебное пособие. М.: Инфра-М, 2013.

3. Вдовин В.М. Предметно-ориентированные экономические информационные системы: учебное пособие. М.: Дашков и К, 2013.

4. Исаев Г.Н. Информационные системы в экономике: Учебник для студентов вузов. М.: Омега-Л, 2013.

5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012.