Этапы создания системы комплексной защиты информации на объекте информатизации
Игошин В. В.

Игошин Вадим Валерьевич / Igoshin Vadim Valer'evich – студент,
кафедра информационной безопасности,
Национальный исследовательский университет Московский институт электронной техники, г. Москва

Аннотация: *в статье описываются цели создания, этапы и особенности разработки, внедрения и эксплуатации системы комплексной защиты информации организации.*

Ключевые слова: *защита информации, система комплексной защиты информации, объект информатизации.*

Информация циркулирует по всей структуре любой организации, что позволяет функционировать огромному количеству процессов. Поэтому главная цель системы комплексной защиты информации организации (СКЗИ) — обеспечение непрерывности процессов, устойчивого функционирования предприятия и предотвращения угроз его безопасности [1]. Понятие СКЗИ предприятия подразумевает совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации (ЗИ) предприятия [1]. Словосочетание *система комплексной* защиты информации объясняется с помощью понятия основной функции предприятия (цели его создания): ее выполнение достигается декомпозицией на более мелкие подфункции; выполнением каждой подфункции занимаются различные отделы организации. С учетом подобной структуры предприятия можно сделать вывод о том, что *система комплексной* защиты информации призвана обеспечивать безопасность информации во всех областях устройства организации, поскольку нарушение одной из них может привести к невозможности дальнейшего функционирования предприятия, вследствие наличия связей и взаимодействий между данными отделами организации.

Для обеспечения защищенности информации на предприятии все сведения, нуждающиеся в защите, в организации выгодно локализовать. Для этого создается объект информатизации (ОИ) - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [2]. Возникает задача обеспечения защищенности не только информационных ресурсов, но и информационных технологий, основных технических средств и систем обработки информации (ОТСС), вспомогательных технических средств и систем (ВТСС), а также помещения, где размещены вышеуказанные элементы объекта информатизации.

Создание СКЗИ объекта информатизации включает в себя три этапа:

1) Анализ объекта информатизации как объекта защиты информации.

Данный этап подразумевает проведение мероприятий, связанных с получением и оценкой исходных данных для создания СКЗИ. К нему относятся: анализ процессов предприятия; определение перечня информации, циркулирующей на объекте информатизации, в том числе и информации ограниченного доступа; анализ ОТСС и ВТСС, структуры автоматизированной системы; создание модели угроз безопасности информации. Оценка полученных данных производится на основе анализа требований нормативно-методических документов и нормативно-правовых актов (в них указаны нормы защищенности информации — качественные и количественные показатели, позволяющие определить требования к обеспечению безопасности информации), регламентирующих защиту информации на объекте информатизации. Итогом этого этапа становится определение несоответствий исходной защищенности информации на ОИ требованиям защиты информации.

2) Разработка СКЗИ объекта информатизации.

Устранение полученных на предыдущем этапе несоответствий осуществляется на данном этапе в четырех направлениях:

- разработка подсистемы физической защиты информации;
- разработка подсистемы защиты информации от утечки по технических каналам;
- разработка подсистемы программно-аппаратной защиты информации;
- разработка подсистемы организационно-правовой защиты информации;

На данном этапе определяются методы и средства защиты информации — устранения существующей уязвимости. Возникает вопрос соотношения эффективности, разрабатываемой СКЗИ, к затрачиваемым средствам на ее создание. Поэтому при разработке СКЗИ одним из основных является принцип разумной достаточности, который подразумевает определение некоторого приемлемого уровня

защищенности информации на ОИ, ведь создать абсолютно защищенную систему невозможно, поскольку при достаточном уровне материального обеспечения и наличии времени можно преодолеть любую защиту. Приемлемой также оказывается разработка сразу нескольких вариантов СКЗИ с различными параметрами.

Таким образом, создание СКЗИ подразумевает разработку и описание решений по каждой подсистеме внедряемой на объект информатизации системы комплексной защиты информации.

3) Внедрение и эксплуатация СКЗИ на объекте информатизации.

На этапе внедрения на основании разработанных технических решений по каждой подсистеме защиты информации осуществляется внедрение СКЗИ: устанавливаются и настраиваются необходимые средства защиты информации, разрабатывается перечень организационно-правовой документации, подготавливается персонал для работы на данном объекте (подготовка необходимых кадров, обучение).

Во время эксплуатации происходят сопроводительные мероприятия по обеспечению защиты информации на ОИ. К ним относятся: своевременное реагирование на возможные угрозы безопасности информации, обновление программного обеспечения, своевременная сертификация средств защиты и продление аттестата соответствия объекта информатизации и прочие.

Создание системы комплексной защиты информации — задача объемная, включающая в себя большое количество нюансов. Однако решение данной задачи позволяет обеспечить безопасность информации, что в большинстве случаев является необходимостью.

Литература

1. *Грибунин В. Г., Чудовский В. В*. Комплексная система защиты информации на предприятии [Текст] - М.: «Академия», 2009 – 416 с.
2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Текст]. – Взамен ГОСТ Р 51275-99; Введ. 2008-02-01 – Москва: Изд-во стандартов, 2007. – 7 с.