Защита курсового проекта на тему «Разработка проекта защиты информации от утечки по техническим каналам в АПК «Астраханский»

Подготовила: студентка гр.ИБ-41 Джантазаева Л. Н.
Преподаватель: Утин М.В.

Защита конфиденциальной информации от утечки по техническим каналам должна осуществляться посредством выполнения комплекса организационных и технических мероприятий, составляющих систему технической защиты информации на защищаемом объекте (СТЗИ), и должна быть дифференцированной в зависимости от установленной категории объекта информатизации или выделенного (защищаемого) помещения.

Организационные мероприятия по защите информации от утечки по техническим каналам в основном основываются на учете ряда рекомендаций при выборе помещений для установки технических средств обработки конфиденциальной информации (ТСОИ) и ведения конфиденциальных переговоров, введении ограничений на используемые ТСОИ, вспомогательные технические средства и системы (ВТСС) и их размещение, а также введении определенного режима доступа сотрудников предприятия (организации, фирмы) на объекты информатизации и в выделенные помещения.

Технические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решений.

При организации работ по защите утечки по техническим каналам информации на защищаемом объекте можно выделить три этапа :

- первый этап (подготовительный, предпроектный);
- второй этап (проектирование СТЗИ);
- третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

Описание деятельности предприятия.

АСТРАХАНСКИЙ
агропромышленный
комплекс

Крупнейшее в России предприятие по производству томатной пасты, расположено на родине томатов - Астраханской области.

Комплекс представляет собой замкнутый цикл от выращивания рассады до производства томатной пасты.

В 2016 году между областным Правительством и ООО «АПК «Астраханский» был заключен инвестиционный договор о присвоении проекту статуса «особо важный инвестиционный проект».

На предприятии задействовано самое современное оборудование итальянской компании ROSSI CATELLI CFT SPA.

Производственные мощности позволяют удовлетворить более 20% спроса на продукцию на территории Российской Федерации.

Предприятие сертифицировано по международной системе FSSC 22000.

На первом этапе осуществляется подготовка к созданию системы технической защиты информации на защищаемых объектах, в процессе которой проводится специальное обследование защищаемых объектов, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

При проведении специального обследования защищаемых объектов с привлечением соответствующих специалистов проводится оценка потенциальных технических каналов утечки информации.

Для анализа возможных технических каналов утечки на объекте изучаются:

- план (в масштабе) прилегающей к зданию местности в радиусе до 150 - 300 м с указанием (по возможности) принадлежности зданий и границы контролируемой зоны;
- поэтажные планы здания с указанием всех помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
- план-схема инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схема системы заземления объекта с указанием места расположения заземлителя;
- план-схема системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схема прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схема систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок.

После проведения предпроектного специального обследования защищаемого объекта группой (комиссией), назначенной руководителем предприятия (организации, фирмы), проводится аналитическое обоснование необходимости создания СТЗИ, в процессе которого:

- определяется перечень сведений, подлежащих защите (перечень сведений конфиденциального характера утверждается руководителем организации);
- проводится категорирование сведений конфиденциального характера, подлежащих защите;
- определяется перечень лиц, допущенных до сведений конфиденциального характера, подлежащих защите;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении и т.п.) информации, характер их взаимодействия между собой и со службой безопасности;
- разрабатывается матрица допуска персонала к сведениям конфиденциального характера, подлежащих защите;
- определяется (уточняется) модель вероятного противника (злоумышленника, нарушителя);
- проводятся классификация и категорирование объектов информатизации и выделенных помещений;
- проводится обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования и внедрения СТЗИ;
- проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;

Результаты аналитического обоснования необходимости создания СТЗИ оформляются пояснительной запиской, которая должна содержать:

- **перечень сведений конфиденциального характера с указанием их уровня конфиденциальности;**
- **перечень сотрудников предприятия, допущенных до конфиденциальной информации, с указанием их режима доступа, а при необходимости и матрицы доступа;**
- **информационную характеристику и организационную структуру объектов защиты;**
- **перечень объектов информатизации, подлежащих защите, с указанием их категорий;**
- **перечень выделенных помещений, подлежащих защите, с указанием их категорий;**
- **перечень и характеристику технических средств обработки конфиденциальной информации с указанием их места установки;**
- **перечень и характеристику вспомогательных технических средств и систем с указанием их места установки;**
- **предполагаемый уровень оснащения вероятного противника (конкурента, злоумышленника);**
- **технические каналы утечки информации, подлежащие закрытию (устранению);**
- **организационные мероприятия по закрытию технических каналов утечки информации;**
- **перечень и характеристику предлагаемых к использованию технических средств защиты информации с указанием их места установки;**
- **методы и порядок контроля эффективности защиты информации;**
- **обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования;**
- **оценку материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;**
- **ориентировочные сроки разработки и внедрения СТЗИ;**
- **перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования СТЗИ.**

Для разработки технического проекта на создание системы технической защиты информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ.

Технический проект СТЗИ содержит:

- **титульный лист;**
- **пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;**
- **перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;**
- **перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;**
- **перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;**
- **перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;**
- **перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;**
- **схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границ контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;**
- **технологические поэтажные планы здания (в масштабе) с указанием мест расположения объектов информатизации и выделенных помещений, характеристик их стен, перекрытий, материалов отделки, типов дверей и окон;**
- **планы объектов информатизации (в масштабе) с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;**
- **план-схему инженерных коммуникаций всего здания, включая систему вентиляции;**
- **план-схему системы заземления объекта, с указанием места расположения заземлителя;**
- **план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;**
- **план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;**
- **план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;**
- **схемы систем активной защиты (если они предусмотрены техническими заданием на проектирование);**
- **инструкции и руководства по эксплуатации технических средств защиты для пользователей и ответственных за обеспечение безопасности информации на объекте информатизации.**

Технический проект согласовывается со службой (специалистом) безопасности заказчика, органа по защите информации проектной организации, представителями подрядных организаций - исполнителей видов работ и утверждается руководителем проектной организации.

На третьем этапе силами монтажных и строительных организаций осуществляется выполнение мероприятий по защите информации, предусмотренных техническим проектом. К работам по монтажу технических средств обработки информации, вспомогательных технических средств, а также проведения технических мероприятий по защите информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ.

Проводится закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка в соответствии с техническим проектом.

Службой (специалистом) безопасности организуется контроль проведения всех мероприятий по защите информации, предусмотренных техническим проектом.

В период установки и монтажа ТСОИ и средств защиты информации особое внимание должно уделяться обеспечению режима и охране защищаемого объекта.

Совместно с представителями проектной и монтажной организаций ответственными за эксплуатацию СТЗИ осуществляется разработка эксплуатационной документации на объект информатизации и выделенные помещения (технических паспортов объектов, инструкций, приказов и других документов).

После установки и монтажа технических средств защиты информации проводится их опытная эксплуатация в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации.

По результатам опытной эксплуатации проводятся приемо-сдаточные испытания средств защиты информации с оформлением соответствующего акта.

В период эксплуатации периодически должны проводиться специальные обследования и проверки выделенных помещений и объектов информатизации. Специальные обследования должны проводиться под легендой для сотрудников организации или в их отсутствие (допускается присутствие ограниченного круга лиц из числа руководителей организации и сотрудников службы безопасности).

Технический проект согласовывается со службой (специалистом) безопасности заказчика, органа по защите информации проектной организации, представителями подрядных организаций - исполнителей видов работ и утверждается руководителем проектной организации.

Заключение

В результате выполнения данного курсового проекта, поставленные цели и задачи были выполнены. Так же была проведена классификация технических каналов утечки информации, были проанализированы возможности перехвата информации по акустическому каналу утечки в выделенном помещении и разработана методика оценки эффективности комплекса защиты по акустическому каналу.

Литература

1. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. – М.: Гротек, 1997, с. 248.
2. Гавриш В.Ф. Практическое пособие по защите коммерческой тайны. – Симферополь: Таврида, 1994, с. 112.
3. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. (Принят и введен в действие Постановлением Госстандарта России от 12 мая 1999 г. № 160).
4. Доктрина информационной безопасности Российской Федерации (Принята 9 сентября 2000 г. № ПР-1895).
5. Организация и современные методы защиты информации. Информационно-справочное пособие. – М.: Ассоциация "Безопасность", 1996, с. 440с.
6. Противодействие экономическому шпионажу: сборник публикаций журнала “Защита информации. Конфидент” 1994 – 2000. – Санкт-Петербург: Конфидент, 2000, с. 344.
7. Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. – Санкт-Петербург: ООО Издательство Полигон, 2000, с. 320.
8. Торокин А.А. Инженерно-техническая защита информации: Учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности. – М.: Гелиос АРВ, 2005, с. 960.
9. Хорев А.А. Способы и средства защиты информации: Учеб. пособие. – М.: МО РФ, 2000, с. 316.