Министерство образования и науки РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

**А.А. Конев, Е.М. Давыдова, А.А. Шелупанов**

# УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

***Методические указания по выполнению практических и самостоятельных работ***

для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность телекоммуникационных систем»,
10.05.03 – «Информационная безопасность автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»
38.05.01 – «Экономическая безопасность»

В-Спектр
Томск, 2017

Практические занятия по дисциплине «Управление информационной безопасностью» заключаются в построении моделей информационных систем, определении элементов информационных систем, подверженных угрозам, и преобразовании структуры информационных систем за счет добавления средств защиты информации, нейтрализующих данные угрозы. Используемые средства – схематичные способы представления систем и процессов, например IDEF0 (рис. 1). Варианты – по согласованию.

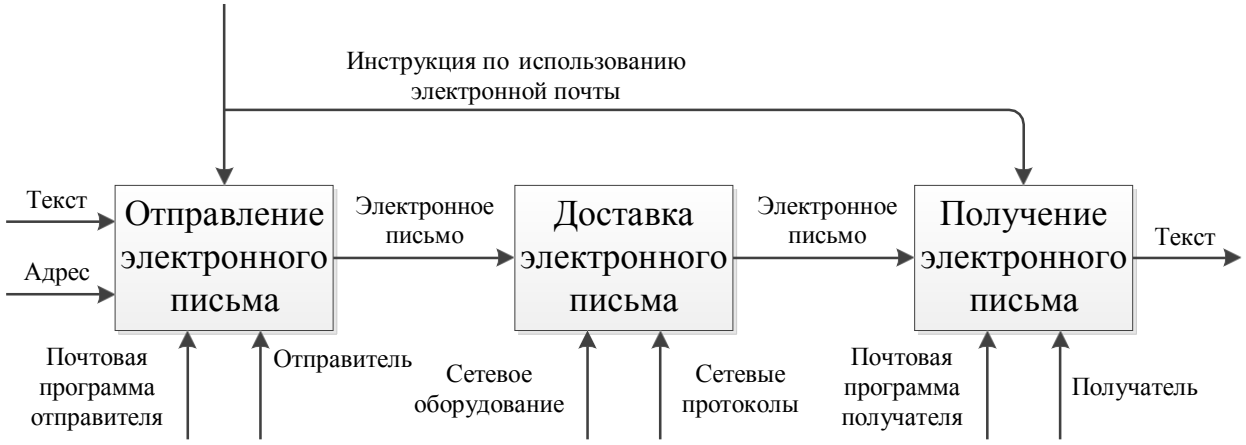


Рисунок 1 – Модель информационной системы «Электронная почта»

Угрозы конфиденциальности выявляются следующим образом – каждому входному элементу, управляющему элементу и механизму должна быть поставлена в соответствие угроза. Перечень угроз, направленных на информационную систему:

- несанкционированный (н/с) текст – отправка запрещенной к передаче конфиденциальной информации (разглашение информации);
- н/с адрес – отправка информации не по адресу получателя (случайно или преднамеренно);
- н/с почтовая программа – использование неразрешенного (например самовольно установленного) программного обеспечения, возможно, зараженного вирусом;
- н/с отправитель – отправка письма от чужого имени, например должностного лица, с указаниями по передаче конфиденциальной

информации («социальная инженерия»);

- н/с инструкция – невыполнение требований инструкции или некорректный инструктаж сотрудника;
- н/с сетевое оборудование – перехват сетевого трафика на сетевом узле, существующем в локальной сети или несанкционированно в нее внедренном;
- н/с сетевые протоколы – использование протоколов, не разрешенных для пересылки конфиденциальной информации (например без шифрования);
- н/с получатель – получение письма человеком, не обладающим допуском к данной информации (например из-за получения чужого пароля к электронной почте).

**Министерство образования и науки Российской Федерации**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)**

Кафедра комплексной информационной безопасности электронно-вычислительных систем

(КИБЭВС)

# ПРИМЕР ОТЧЕТА

по практической работе

по дисциплине «Управление информационной безопасностью»

Выполнили:

студенты гр. 7__

_____

_____

Принял:

_____ _____

_____

Томск 2016

## Введение

Цель работы: описать информационный процесс, рассмотреть угрозы, выбрать организационные и технические средства защиты.

## Ход работы


Рисунок 1 – Разбор информационного процесса, черный ящик

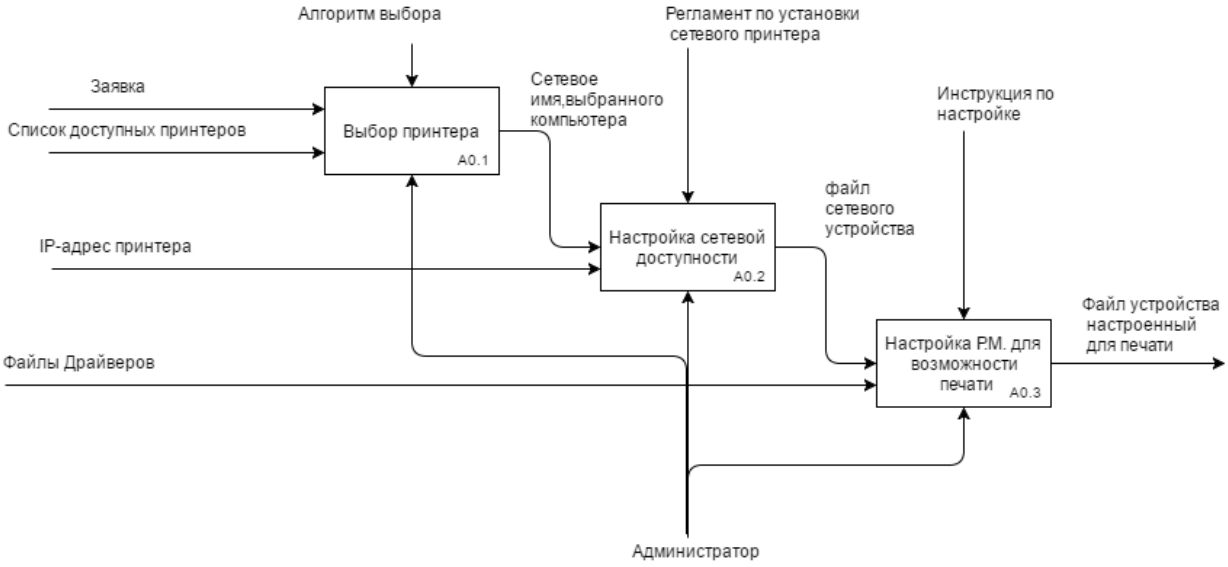


Рисунок 2 – Разбор информационного процесса, декомпозиция черного ящика

Таблица 1 – Угрозы и средства защиты

| Под процесс | Угрозы | Средства Защиты |
|---|---|---|
| Заявка | Конфиденциальности: разглашение информации о заявке в электронном виде (информация о грифе печатных документов); | Орг: Подписка о неразглашении, разграничение доступа к завявке. |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование, |
| | Целостность: Подмена личности указанной в заявке; | Орг: Разграничение доступа; |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование; |
| Список доступных принтеров | Конфиденциальность:-; | Орг:-; |
| | | Тех: -; |
| | Целостность: Удаление\изменение ; | Орг: разграничение доступа к списку доступных принтеров; |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование. |
| IP –адрес принтера | Конфиденциальность: раскрытие ip-адреса; | Орг: Подписка о неразглашении, разграничения доступа к управления настройками сети. |
| | | Тех: Фильтрация трафика исходящего, входящего, сегментация внутренней сети, настройка Access листов, установка единственного IP адреса во внешнею сеть; |
| | Целостность: подмена ip-адреса; | Орг: разграничение доступа к управления настройками сети; |
| | | Тех: Фильтрация трафика исходящего, входящего, сегментация внутренней сети, периодическая проверка MAC адресов в выбранном сегменте, настройка Access листов; |
| Файлы драйверов | Конфиденциальность: разглашение версии драйвера; | Орг: Подписка о неразглашении. |
| | | Тех: -; |
| | Целостность: модификация драйвера | Орг: Разграничения |

| | | |
|---|---|---|
| | злоумышленником; | доступа к управлению настройками системы. |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование. |
| Алгоритм выбора | Конфиденциальность: раскрытие списка секретных принтеров; | Орг: Подписка о неразглашении, инструкция правильного использования алгоритма выбора принтера; |
| | | Тех: -; |
| | Целостность: удаление\изменение алгоритма выбора; | Орг: Инструкция об использовании алгоритма |
| | | Тех: Аудит на добавление принтера; |
| Регламент по установке сетевого принтера | Конфиденциальность: разглашение информации о регламенте; | Орг: Подписка о неразглашении, разграничение доступа к регламенту; |
| | | Тех: -; |
| | Целостность: удаление\изменение регламента; | Орг: Разграничение доступа к регламенту; |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование; |
| Инструкция по настройки принтера | Конфиденциальность: разглашение информации по инструкции; | Орг: Подписка о неразглашении, разграничение доступа к инструкции; |
| | | Тех: -; |
| | Целостность: удаление\изменение инструкции; | Орг: Разграничение доступа к инструкции; |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование; |
| Сетевое имя выбранного компьютера | Конфиденциальность: разглашение информации о сетевом имени компьютера; | Орг: Подписка о неразглашении; |
| | | Тех:-; |
| | Целостность: удаление\изменение сетевого имени компьютера; | Орг: Разграничение доступа к настройкам сети; |
| | | Тех: Реализация разграничения доступа; |
| Файл сетевого устройства | Конфиденциальность: разглашение информации о файле сетевого устройства; | Орг: Подписка о неразглашении, |
| | | Тех: -; |

| | | |
|---|---|---|
| | Целостность: удаление\изменение файла сетевого устройства; | Орг: Разграничение доступа к управлению настройками сети; |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование; |
| Администратор | Конфиденциальность: разглашение информации об администраторе; | Орг: Подписка о неразглашении, разграничение доступа к персональным данным администратора |
| | | Тех: - |
| | Целостность: урон от болезни здоровью администратора с последующим выходом из строя администратора. | Орг: Периодическое обследование сотрудников, вакцинация сотрудников; |
| | | Тех: -;. |
| Файл устройства, настроенный для печати | Конфиденциальность: разглашение информации о файле устройства настроенного для печати | Орг: Подписка о неразглашении. |
| | | Тех: -;. |
| | Целостность: удаление\изменение файла устройства настроенного для печати. | Орг: Разграничение доступа к настройкам системы. |
| | | Тех: Периодическая проверка контрольных сумм файлов, резервное копирование;. |

**Заключение**

В практическом задании был рассмотрен информационный процесс «Получение доступа к сетевому принтеру для печати», были выделены угрозы, а также применены организационные и технические средства защиты к ним.