М.С. АЛЕКСЕЕНКО, студентка гр. КЗИ-110;
Д.В. МИШИН, ст. преподаватель, к.т.н.

ОБ АДМИНИСТРАТОРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ

В работе представлен анализ текущих публикаций, а также технической документации. Рассмотрены основные термины и определения телекоммуникационной сети и ее компонентов. Выявлены показатели администратора информационной безопасности как компонента автоматизированной системы.

Ключевые слова: администратор информационной безопасности, автоматизированная система, телекоммуникационная сеть.

0 рис., 0 табл., 8 источников.

Телекоммуникационная сеть предприятия работает под управлением администратора. Наличие угроз безопасности всевозможных видов утечек ставит под угрозу деятельность сети, поэтому функционирование невозможно без администратора безопасности. Определение эффективности является решающим для обеспечения эффективной работы АС.

Деятельность администратора непосредственно связана с:

- выполнением правил эксплуатации средств защиты информации;
- обеспечением непрерывности процесса обработки информации;
- реагированием на нарушения в компьютерной системе и восстановлением работоспособности компьютерной системы;

Объектом исследования является администратор информационной безопасности телекоммуникационной сети предприятия.

Предмет исследования – модели администратора информационной безопасности телекоммуникационной сети предприятия как ЧМС.

На данном этапе работы ставились следующие задачи:

- анализ публикаций, содержащих актуальные результаты в исследуемой области; стандартов ГОСТ, ИСО; методических рекомендаций и документов;
- выявление показателей администратора ИБ ТС автоматизированной системы.

В ходе первого этапа работы, необходимого для составления модели администратора ИБ, были достигнуты следующие результаты:

1. Проанализирована техническая документация, связанная с работой автоматизированных систем, приведенная ниже:

- ГОСТ Р МЭК 60447-2000. ИНТЕРФЕЙС ЧЕЛОВЕКО-МАШИННЫЙ. Принципы приведения в действие.

- ГОСТ 34.003-90. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. Термины и определения.

- ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении»

- ГОСТ 26378-84 Система «Человек-машина». Термины и определения

- НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, Часть 1, Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

2. В результате анализа отобранных источников раскрыты понятия автоматизированных систем и администратора информационной безопасности с точки зрения технической документации по работе АС.

Рассмотрение предметной области началось с понятия «телекоммуникационная система». Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Наличие средств вычислительной техники и, соответственно, персонала, обращающейся к ней, говорит о том, что ТС – составляющая автоматизированной системы предприятия.

В рамках данной работы решено рассматривать автоматизированную систему как совокупность персонала и средств автоматизации деятельности, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

В технической документации по АС отсутствует определение

администратора. Поэтому к нему придем через определение оператора АС.

Персонал автоматизированной системы в общем случае это оператор. Понятие администратора является подмножеством оператора. Различие – в функциях: у администратора функций управления системой, в частности у администратора ИБ – защита от несанкционированного доступа к информации.

Приходим к выводу, что администратор информационной безопасности – это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

3. Определены функции администратора ИБ.

В результате анализа ГОСТ 34.003-90. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. Термины и определения и методического документа ФСТЭК «Меры защиты информации в государственных информационных системах» было выделено множество функций администратора информационной безопасности:

F1. Обеспечение функционирования средств и систем защиты информации в пределах инструктивно-методических документов

F2. Обучение персонала и пользователей вычислительной техники правилам безопасной обработки информации и правилам работы со средствами защиты информации.

F3. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

F4. Текущий контроль технологического процесса автоматизированной обработки информации ограниченного распространения и электронных платежных документов.

F7. Выбор модели разграничения доступа, внедрение и сопровождение.

F8. Ведение журнала информационной безопасности.

F9. Создание и поддержание в актуальном состоянии пользовательских учётных записей.

F10. Обслуживание систем идентификации/аутентификации.

F11. Резервное копирование и архивирование

Задача эффективной деятельности администратора в автоматизированной системе сложна и имеет существенную важность. В этом взаимодействии есть множество слабых мест, как со стороны человека, так и со стороны технического обеспечения.

4. Выявлены некоторые показатели администратора информационной безопасности автоматизированной системы.

Администратор не огражден от своих ошибок, а также подвержен внешнему влиянию неблагоприятных факторов. Это может привести к сбоям в работе автоматизированных систем.

В книге «Предоставление информации оператору» Галактионов строит модели деятельности оператора АС в зависимости от уровня знаний, его натренированности и знания вероятности событий.

Сложным системам присущи различные свойства, но среди них есть такие, которыми нельзя пренебрегать, исследуя их функционирование, прогнозируя развитие, анализируя их взаимодействие с внешней средой. Поскольку администратор ИБ – компонент АС, то будем рассматривать его показатели как для автоматизированной системы.

Показатели :

- эффективность
- производительность
- работоспособность
- устойчивость

  - живучесть,

  -надежность,

  -отказоустойчивость.

Производительность администратора – это возможность (или способность) выполнения своих функций на согласованном уровне при установленных параметрах нагрузки на автоматизированную систему.

Эффективность администратора - свойство, характеризуемое степенью достижения целей, связанных с обеспечением информационной безопасности на предприятии.

Работоспособное состояние администратора - состояние, при котором он способен осуществлять свои функции с требуемым качеством.

Живучесть администратора - способность адаптироваться к новым условиям работы, противостоять нежелательным влияниям при одновременной реализации основной функции.

Отказоустойчивость администратора — свойство сохранять работоспособность в случае отказа одной или нескольких компонент автоматизированной системы.

Надежность администратора – это свойство выполнять заданные функции в течение определенного времени при заданных условиях работы.

Если компенсация ошибок оператора и отказов техники невозможна, то вероятность безотказной работы системы:

$$P_1(t_0,t) = P_T(t_0,t)P_0(t)$$

где $P_T(t_0,t)$ - вероятность безотказной работы технических средств в течении времени $(t_0,t,+t)$

$P_0(t)$ – вероятность безошибочной работы оператора в течении времени, при условии, что техника работает безотказно

t_0 - общее время эксплуатации системы

t – рассматриваемый период работы.

Совокупность приведенных выше показателей используется для оценки автоматизированной системы.

В дальнейшем планируется:

- Классифицировать модели оператора АС.
- Выработать критерии выбора существующих моделей в рамках решаемой задачи.
- Выбрать из существующих моделей наиболее применимые для

моделирования администратора информационной безопасности автоматизированной системы.

Литература

1. ГОСТ Р МЭК 60447-2000. ИНТЕРФЕЙС ЧЕЛОВЕКО-МАШИННЫЙ. Принципы приведения в действие.

2. ГОСТ 34.003-90. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. Термины и определения.

3. ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении»

4. ГОСТ 26378-84 Система «Человек-машина». Термины и определения

5. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, Часть 1, Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

6. Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов города Москвы Москва, 2006 г

7. *А.М. Цыбулин* ПОДХОД К ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ, Вестник ВолГУ. Серия 10. Вып. 5. 2011

8. *П.Н. Девянин* Модели безопасности компьютерных систем, 2005г