Министерство науки и высшего образования 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)

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ И КАТЕГОРИИ НАРУШИТЕЛЕЙ

Практическая работа по дисциплине

«Катастрофоустойчивость автоматизированных банковских систем»

Выполнил

студент гр. 728-2

\_\_\_\_\_\_\_\_Геворгян Д.Р.

Проверил старший преподаватель

кафедры КИБЭВС

\_\_\_\_\_\_\_\_\_ Кочетков О. В.

Томск 2021

1 Введение

В данной работе необходимо на основании положений Рекомендаций РС БР ИББС - 2.9-2016, исходя из назначенных ролей указать виды защищаемой информации, к которой имеется доступ, типы используемых информационных активов и объектов среды информационных активов, перечень категорий возможных внутренних нарушителей с которыми возможно взаимодействие (ранжированный по частоте такого взаимодействия).

2 Ход работы

Выданная роль – руководитель отдела ИТ.

2.1 Виды защищаемой информации, к которой имеется доступ

Категории информации были взяты из РС БР ИББС-2.9-2016, Приложение А [1].

– информация о предоставленных правах доступа к АБС организации БС РФ.

– техническая документация на программные компоненты, используемые в организации БС РФ, включая исходные коды программных компонентов.

– информация о конкретных методах или способах обеспечения безопасности и защиты информации в организации БС РФ.

– персональные данные партнеров и клиентов организации БС РФ.

– персональные данные работников организации БС РФ.

2.2 Типы используемых информационных активов и объектов среды информационных активов

Информация взята из раздела 7 (Рекомендации к реализации идентификации и учета информационных активов информации конфиденциального характера и объектов среды информационных активов, используемых для обработки информации конфиденциального характера) РС БР ИББС-2.9-2016.

Типы информационных активов:

– персональные данные;

– виртуальные машины, предназначенные для размещения автоматизированных рабочих мест пользователей и эксплуатирующего персонала;

Типы объектов среды информационных активов:

– рабочие станции пользователей;

– переносные (портативные) средства вычислительной техники (например, ноутбуки, планшетные компьютеры, смартфоны);

– переносные носители информации (например, CD/DVD/blu-ray-диски, флеш-память, карты памяти, внешние HDD-диски, магнитные ленты);

– бумажные носители информации.

Для каждого информационного актива рекомендуется обеспечивать хранение как минимум следующих учетных данных:

– данные, позволяющие установить средство вычислительной техники - объект среды информационного актива;

– данные, определяющие владельца информационного актива.

Для каждого средства вычислительной техники - объекта среды информационных активов рекомендуется обеспечивать хранение как минимум следующих учетных данных:

– данные, позволяющие идентифицировать средство вычислительной техники;

– данные, позволяющие установить место физического размещения средств вычислительной техники;

– перечень информационных активов, размещенных на средстве вычислительной техники;

– данные, позволяющие идентифицировать логическое размещение средства вычислительной техники, например сетевой адрес, доменное имя;

– данные, устанавливающие тип вычислительной техники;

– данные, устанавливающие класс информации конфиденциального характера, размещенной на средстве вычислительной техники.

2.3 Перечень категорий возможных внутренних нарушителей

Информация взята из раздела 8 (Рекомендации к определению категорий возможных внутренних нарушителей и потенциальных каналов утечки информации) РС БР ИББС-2.9-2016.

Ранжированный по частоте взаимодействия перечень категорий возможных внутренних нарушителей для выданной роли (от самого частого до менее):

1. Категория А2*.*Пользователь (большинство работников организации БС РФ).
2. Категория Б. Эксплуатационный персонал - лица, в том числе не являющиеся работниками организации БС РФ, обладающие возможностями по доступу к информации конфиденциального характера при осуществлении задач, связанных с эксплуатацией и (или) администрированием информационной инфраструктуры организации БС РФ, АБС и приложений организации БС РФ;
3. Категория А1*.* Доверенный пользователь (например, высшее руководство организации БС РФ).
4. Категория А3*.* Пользователь "в зоне риска" (например, работники организации БС РФ на испытательном сроке, подавшие заявление на увольнение или ранее участвовавшие в инцидентах ИБ).
5. Категория В*.* Технический и вспомогательный персонал - лица, в том числе не являющиеся работниками организации БС РФ, не обладающие полномочиями по доступу к информации конфиденциального характера, но осуществляющие непосредственный физический доступ в помещения, в которых осуществляется обработка такой информации;
6. Категория Г. Лица, не являющиеся работниками организации БС РФ, обладающие доступом к информации конфиденциального характера на основании договорных отношений (например, аудиторы, партнеры и подрядчики), требований законодательства Российской Федерации (например, органы государственной власти) и (или) судебного решения.

3 Заключение

В ходе выполнения данной работы на основании положений Рекомендаций РС БР ИББС - 2.9-2016, исходя из назначенной роли были указаны виды защищаемой информации, к которой имеется доступ, типы используемых информационных активов и объектов среды информационных активов, а также составлен перечень категорий возможных внутренних нарушителей, с которыми возможно взаимодействие (ранжированный по частоте такого взаимодействия).

Список использованной литературы

# 1 РС БР ИББС-2.9-2016 27.07.2006 [Электронный ресурс] – Режим доступа <https://cbr.ru/Crosscut/LawActs/File/445>