Воздвиженская Надежда, группа 6015 (3 вариант)   
Активы соответствующие 3 варианту

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3 вар. | 7 | 10 | 17 | 28 | 31 | 38 | 1700 |

**Выбор актива на основе варианта**

**7** Банковский технологический процесс генерации отчетов для ЦБ РФ (выполняется в отделении по работе с юридическими лицами).

**10** Системная документация по АСУ, программному обеспечению, операционным системам.

**17** Активы программного обеспечения (инсталляции и установленное ПО): операционные системы прикладное программное обеспечение, АСУ банковскими процессами, системное программное обеспечение, инструментальные средства разработки и утилиты

**28** Автоматизированная банковская система (АБС), обеспечивающая реализацию основных функций банковских технологических процессов по работе с клиентами при выполнении различных банковских услуг (кредиты, депозиты, ценные бумаги и др. операции). Клиентская база данных относится к банковской тайне. Ответственность за информацию – персональная для сотрудников, имеющих доступ к АБС. Ответственность за работу АСУ – инженер АСУ.

**31** Отчетные материалы бухгалтерской отчетности и другие сведения о деятельности банка, доступные для всех. Ответственный – бухгалтер.

**38** Персональные данные сотрудников и клиентов банка (электронная и бумажная форма) хранятся в кабинете управляющего. В электронном виде эта информация доступна только для управляющего банка и его заместителю.

**Угрозы для активов**

|  |  |  |
| --- | --- | --- |
| **№** | **Категория угроз** | **Наименование уязвимостей системы ИБ, выявленных при аудите** |
| **7** | ФБ | Размещение и оборудование рабочих мест допускает возможность допуска к АРМ посторонних лиц |
| **10** | ФБ | Во всех помещения используются установки автоматического водяного пожаротушения, это может привести к выводу из строя оборудования |
| **17** | ЭИС | Антивирусные программы используются не на всех рабочих местах. Обновления баз данных сигнатур делается самостоятельно на каждом рабочем месте. |
| **28** | ОБ | Бумажные носители информации с ошибками оформления договоров, копии документов не уничтожались, а выбрасывались в мусорные корзины |
| **31** | ОБ | Внешний аудит системы информационной безопасности не проводился. |
| **38** | ОБ | В помещениях, где проводится обработка конфиденциальной информации (банковской тайны) не обеспечена защита от утечки информации. |

Обозначения:

* ФБ-физическая защита;
* ОБ-организация защиты;
* КБ-кадровые вопросы безопасности;
* УД-управление доступом;
  + - П-политика безопасности;
    - ЭИС-эксплуатация информационных систем.

# **Инвентаризация и классификация информационных** **активов (этап1)**

В ходе выполнения этого этапа будут определены приоритеты активов по их ценности.

Модель классификации информационных активов необходимо представить в форме кортежа <***A, F, H, V>***

**Актив № 7**

**1.Наименование:** Банковский технологический процесс генерации отчетов для ЦБ РФ (выполняется в отделении по работе с юридическими лицами).

**1.2. Форма представления актива:**

-электронная;

- бумажная.

**1.3. Ценность актива** – *Критичная* (Банковская тайна, данные о поступлениях средств, данные о вкладах).

**1.4. Владелец актива:**

* Ведущий специалист по работе с юридическими лицами (начальник отдела) (отправляет электронный отчет в ЦБ РФ)
* Инженер АСУ банка (за обеспечение конфиденциальности, целостности и доступности к АСУ).
* Бухгалтера (генерируют отчет)

**Актив № 10**

**1.Наименование:** Системная документация по АСУ, программному обеспечению, операционным системам.

**1.2. Форма представления актива:**

* *программное обеспечение*

**1.3. Ценность актива**

* *Высокая* (неисправность приведет парализации работы банка).

**1.4. Владелец актива:**

* инженер АСУ

**Актив № 17**

**1.Наименование:** Активы программного обеспечения (инсталляции и установленное ПО): операционные системы прикладное программное обеспечение, АСУ банковскими процессами, системное программное обеспечение, инструментальные средства разработки и утилиты.

**1.2. Форма представления актива:**

* программное обеспечение*;*

**1.3. Ценность актива** – высокая (неисправность приведет парализации работы банка).

**1.4. Владелец актива:**

* Инженер АСУ (системный администратор) (Отвечает за функционирование программно-аппаратного обеспечения)

**Актив № 28**

**1.Наименование:** Автоматизированная банковская система (АБС), обеспечивающая реализацию основных функций банковских технологических процессов по работе с клиентами при выполнении различных банковских услуг (кредиты, депозиты, ценные бумаги и др. операции). Клиентская база данных относится к банковской тайне. Ответственность за информацию – персональная для сотрудников, имеющих доступ к АБС. Ответственность за работу АСУ – инженер АСУ

**1.2. Форма представления актива:**

* программное обеспечение

**1.3. Ценность актива**–*Критичная* (При выходе из строя программного обеспечения, деятельность банка будет парализована частично, либо полностью, если из строя выйдут ключевые узлы программного обеспечения, например, операционная система на сервере базы данных)

**1.4. Владелец актива:**

* инженер АСУ

**Актив № 31**

**1.Наименование:** Отчетные материалы бухгалтерской отчетности и другие сведения о деятельности банка, доступные для всех.

**1.2. Форма представления актива:**

* бумажная

**1.3. Ценность актива** – высокая (Банковская тайна, данные о поступлениях средств, данные о вкладах).

**1.4. Владелец актива:**

* Бухгалтера (Работают с бумажными документами необходимыми для генерации отчета

**Актив № 38**

**1.Наименование:** Персональные данные сотрудников и клиентов банка (электронная и бумажная форма) хранятся в кабинете управляющего. В электронном виде эта информация доступна только для управляющего банка и его заместителю.

**1.2. Форма представления актива:**

* электронная

**1.3. Ценность актива** – Критичная (банковская тайна, организационные документы, личные данные клиентов, номера счетов)

**1.4. Владелец актива:**

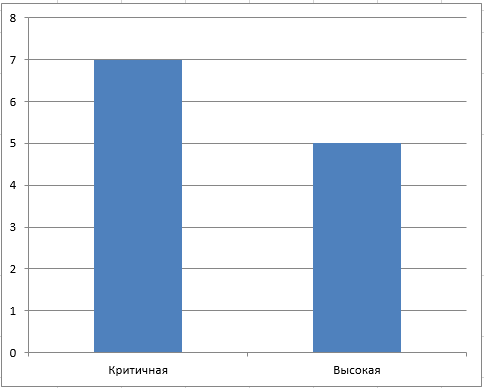
* инженер АСУ
* специалист по информационной безопасности

*Таблица 1.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Номер актива** | **Форма** | **Владелец** | **Ценность** |
| **1** | 7 | ПО | Инженер АСУ | Критичная |
| **2** | 10 | ПО | Инженер АСУ | Высокая |
| **3** | 17 | ПО | Инженер АСУ  Специалист по информационной безопасности | Высокая |
| **4** | 28 | ПО | инженер АСУ | Критичная |
| **5** | 31 | бумажная | Бухгалтера | Высокая |
| **6** | 38 | электронная | инженер АСУ , специалист по информационной безопасности | Критичная |

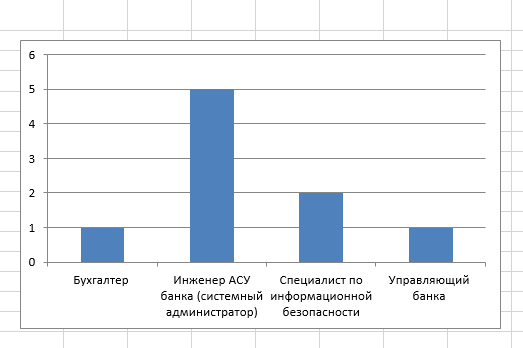
Проанализировав получившиеся данные, можно сделать вывод, что активы под номерами 7, 28 и 38 являются критичными. Активы под номерами 10,17,31 были назначены активами высокой ценности. На рис. 1 представлена гистограмма распределения активов по ценности.

На основе критериев оценки влияния риска на бизнес-процессы, был построен график (см. рис. 1).



*Рис. 1. Распределение активов по ценности*

Так же на основании анализа данных можно составить гистограмму по ответственным за активы лицам (см. рис. 2).



*Рис 2. Распределение активов по ответственным лицам.*

Проанализировав данную диаграмму можно сделать вывод о том, что наибольшая ответственность за представленные активы ложиться на плечи инженера АСУ банка, ведь 5 активов из 6 затрагивают непосредственно АСУ. За ним идет специалист по информационной безопасности, в его зону ответственности попадает 2 актива, и по одному активу распределяется между Ведущим специалистом по обслуживанию юридических лиц, бухгалтерами и управляющим банком.

Таким образом, представляется наиболее полная картина распределения активов по степени угроз и по ответственным лицам, пересечение гистограмм говорит о том, что все критические угрозы находятся в зоне ответственности инженера АСУ, что говорит о большой доле уязвимостей так или иначе связанных с информационными технологиями.