# **Модернизированный раздел угроз БДУ ФСТЭК.**

**11 глобальных угроз:**

[**УБИ.1 Угроза утечки информации**](https://bdu.fstec.ru/threat-section/threats/УБИ.1)

#### [УБИ.2 Угроза несанкционированного доступа](https://bdu.fstec.ru/threat-section/threats/УБИ.2)

#### [УБИ.3 Угроза несанкционированной модификации (искажения)](https://bdu.fstec.ru/threat-section/threats/УБИ.3)

#### [УБИ.4 Угроза несанкционированной подмены](https://bdu.fstec.ru/threat-section/threats/УБИ.4)

#### [УБИ.5 Угроза удаления информационных ресурсов](https://bdu.fstec.ru/threat-section/threats/УБИ.5)

#### [УБИ.6 Угроза отказа в обслуживании](https://bdu.fstec.ru/threat-section/threats/УБИ.6)

#### [УБИ.7 Угроза ненадлежащего (нецелевого) использования](https://bdu.fstec.ru/threat-section/threats/УБИ.7)

#### [УБИ.8 Угроза нарушения функционирования (работоспособности)](https://bdu.fstec.ru/threat-section/threats/УБИ.8)

#### [УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника](https://bdu.fstec.ru/threat-section/threats/УБИ.9)

#### [УБИ.10 Угроза распространения противоправной информации](https://bdu.fstec.ru/threat-section/threats/УБИ.10)

#### [УБИ.11 Угроза несанкционированного массового сбора информации](https://bdu.fstec.ru/threat-section/threats/УБИ.11)

У каждой угрозы есть карточка с описанием, возможные объекты воздействия, возможные способы реализации.

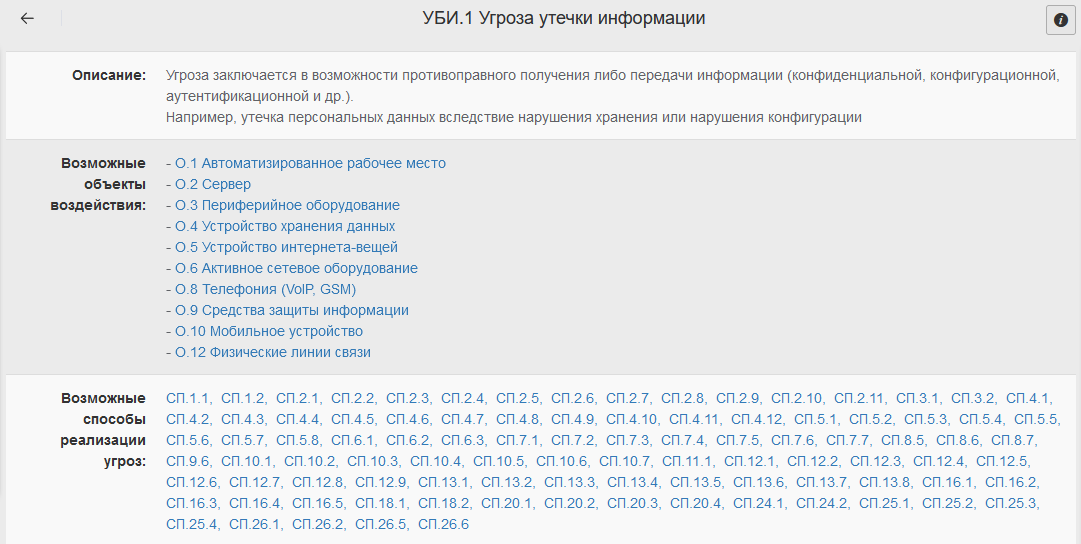


Рис. 1 – Карточка УБИ.1 Угроза утечки информации

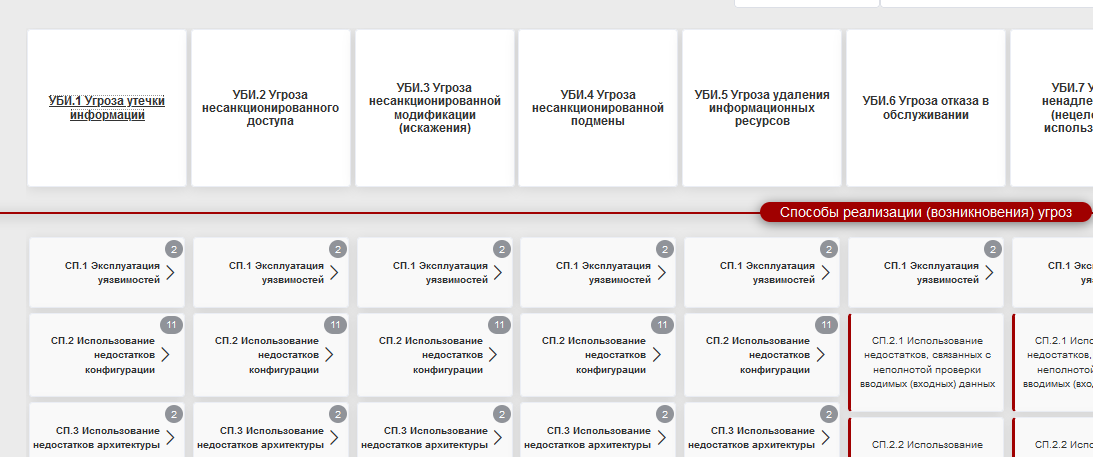
На сайте это представлено в следующем виде – сверху угрозы, снизу релевантные способы реализации угроз.  


Рис. 2 – Представление угроз и способов их реализации

Банк представлен следующими справочниками:

- Негативные последствия:

Представляет собой комбинацию ущерба и угроз (УБИ) с ним связанных.  
Ущерб:

- Физическому лицу

- Риски юридическому лицу, индивидуальному предпринимателю, связанный с хозяйственной деятельностью

- Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности

Всего 52 негативных последствия.

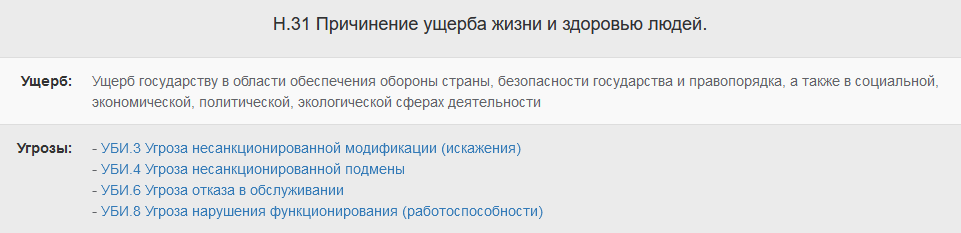


Рис.3 – Пример негативного последствия

- Угрозы

Общие угрозы информационной безопасности.

Всего 11 угроз.

- Объекты воздействия

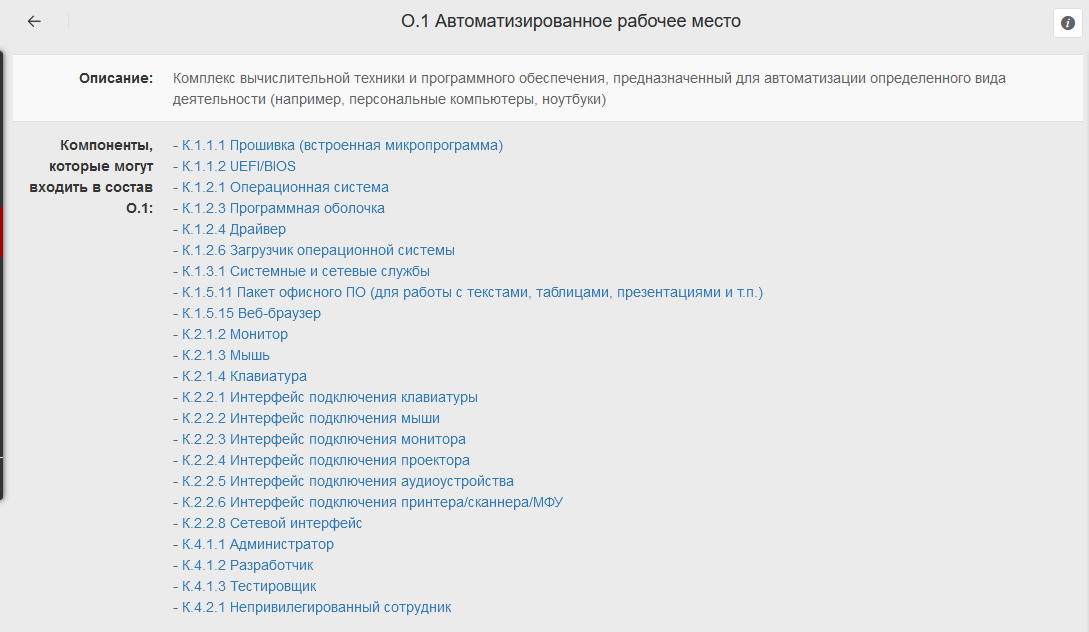
Обобщённые объекты воздействия, состоят из описания и возможных компонентов объекта.

Рис.4 – Пример объекты воздействия

- Компоненты

Составляющие объектов воздействия.

- Способы реализации

Возможные способы реализации угроз. Делятся на 26 групп, в которых содержатся более конкретные описания реализаций угроз (уровень возможностей нарушителя, возможные реализуемые угрозы, компоненты объектов воздействия, возможные меры защиты).

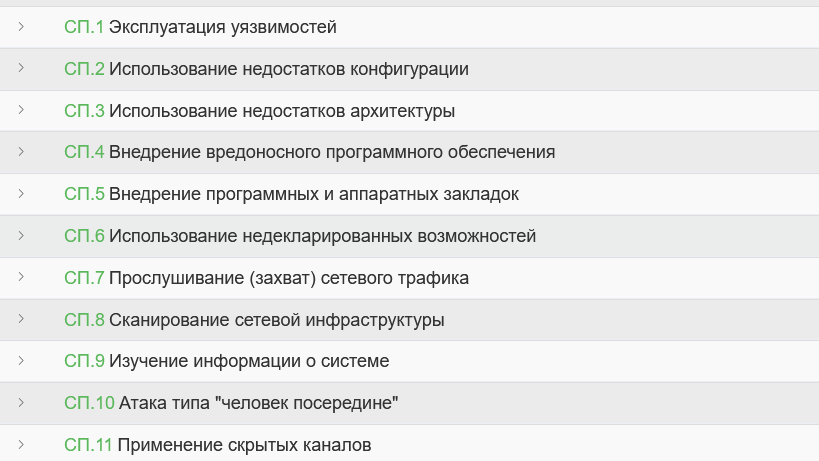


Рис. 5 – Группы способов реализации угроз, ч.1

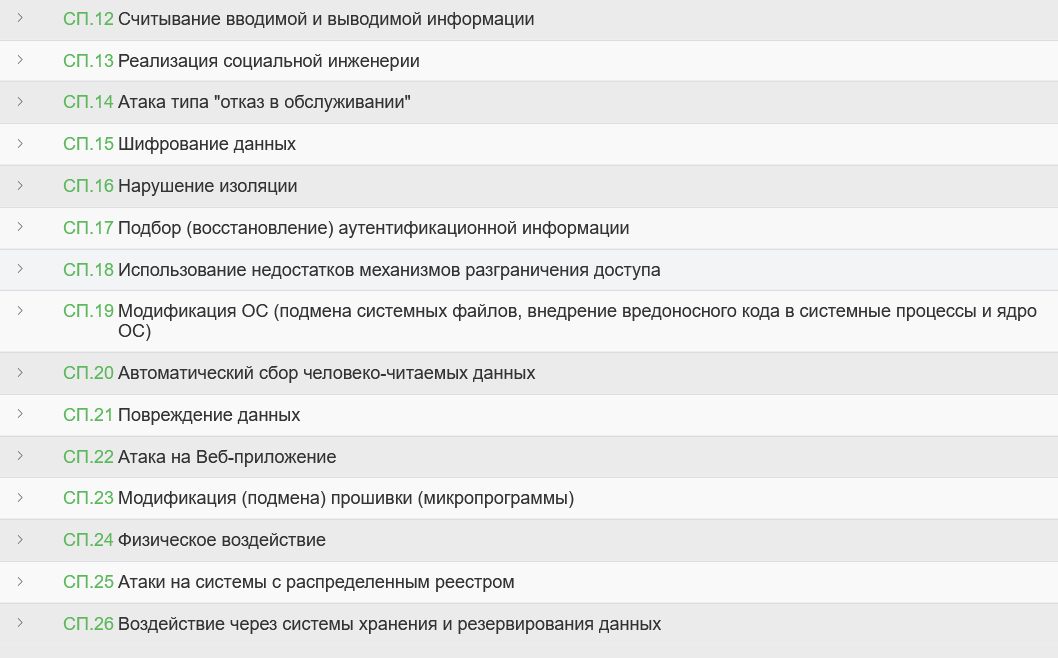


Рис. 6 – Группы способов реализации угроз, ч.2

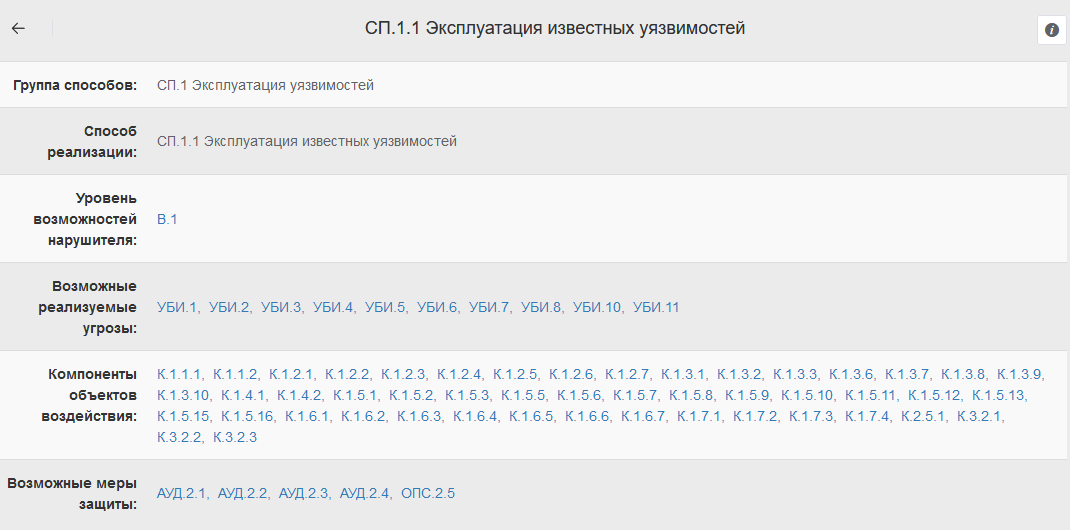


Рис. 7 – Пример карточки способа реализации угроз

- Нарушители

4 типа уровня возможностей нарушителей:

- Нарушитель, обладающий базовыми возможностями

- Нарушитель, обладающий базовыми повышенными возможностями

- Нарушитель, обладающий средними возможностями

- Нарушитель, обладающий высокими возможностями

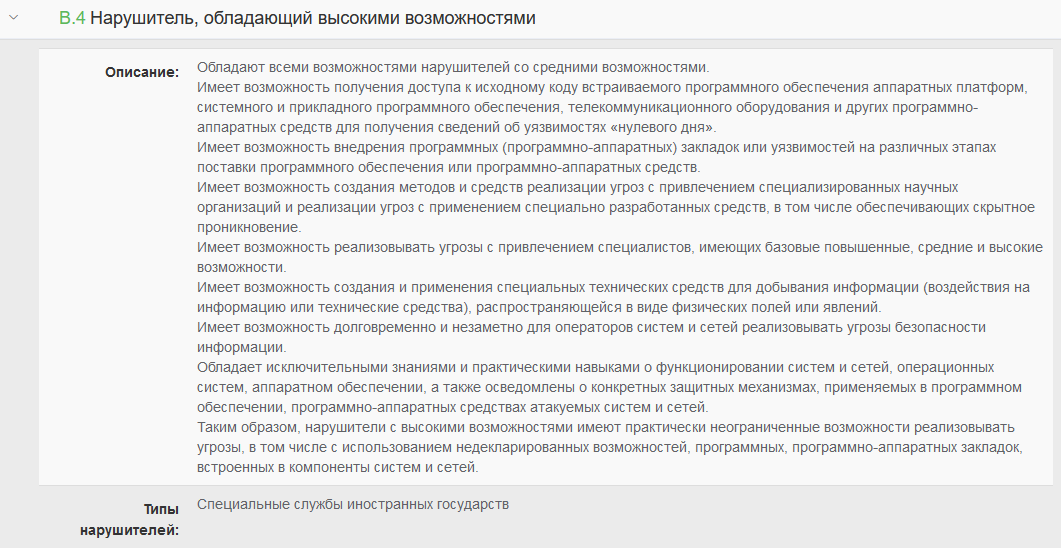


Рис. 8 – Пример карточки уровня возможности нарушителя

- Меры защиты

Обширное количество мер защиты информации, которые делятся на группы и подгруппы, сокращения сделаны из названий групп.

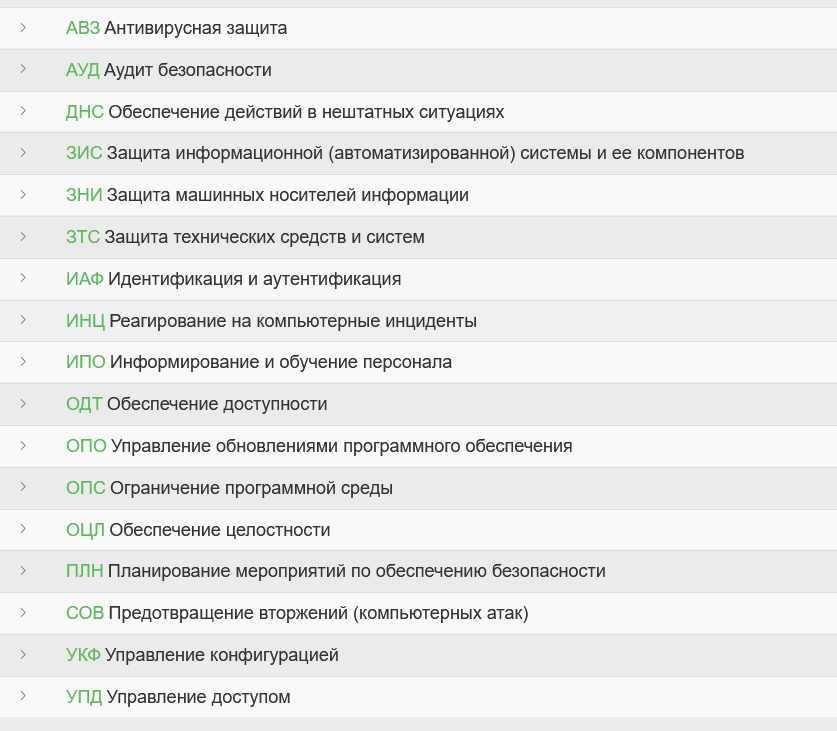


Рис. 9 – Группы мер защиты информации

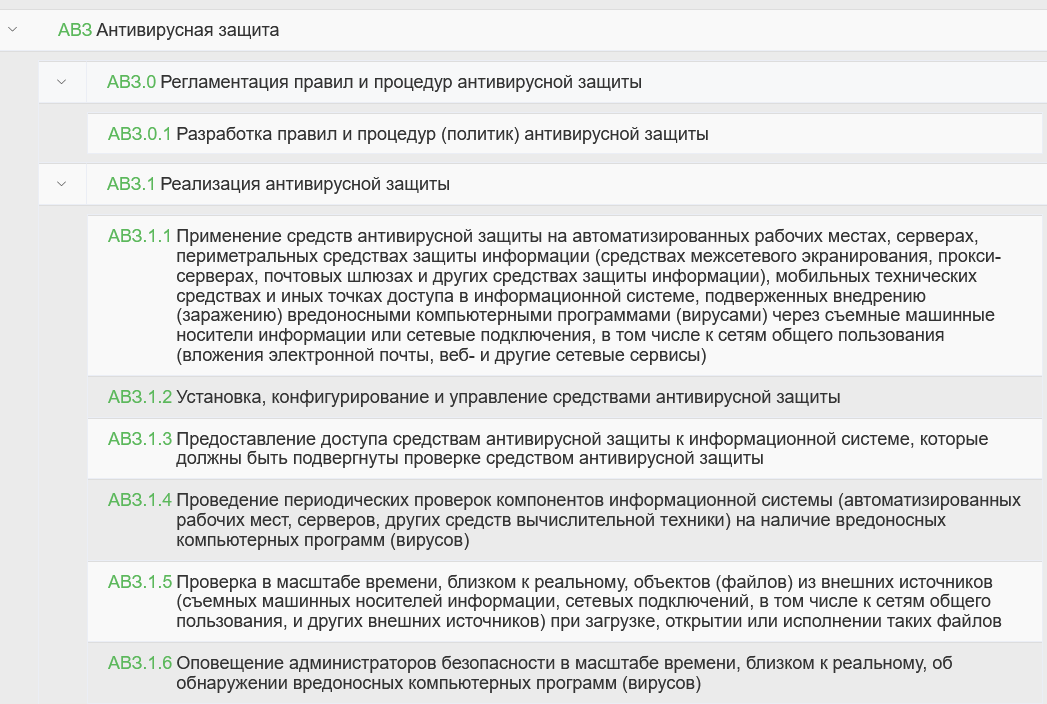


Рис. 10 – Пример деления на подгруппы

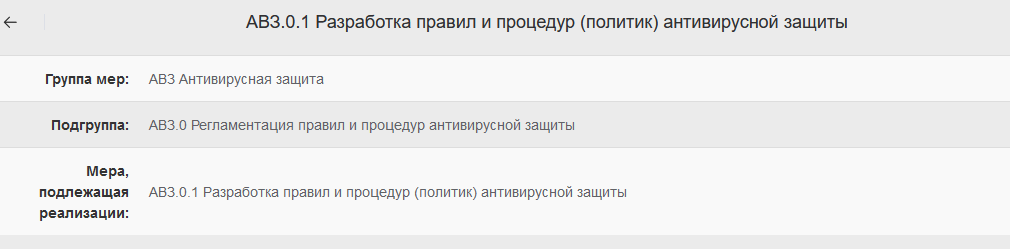


Рис. 11 – Пример карточки меры

# **Формирование перечня возможных угроз информационной безопасности.**

На сайте присутствует раздел, который призван помочь работнику в сфере информационной безопасности определить перечень возможных УБИ, а также определить меры защиты для защищаемых объектов на основе информации в справочниках.



Рис. 12 – Схема формирования перечня возможных УБИ

Определение перечня возможных угроз происходит в интерактивном режиме: исходя из выбранных негативных последствий, автоматически определяются возможные угрозы, хотя есть возможность выбрать их самостоятельно.

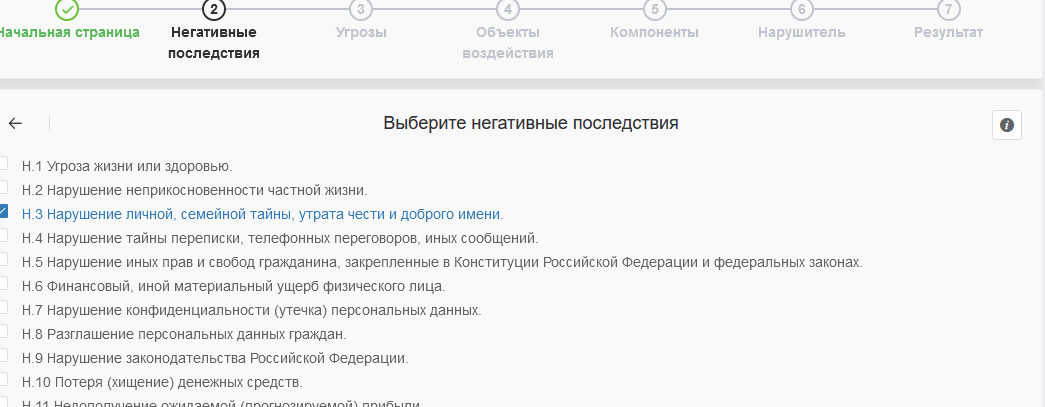


Рис. 13 – Выбор негативных последствий

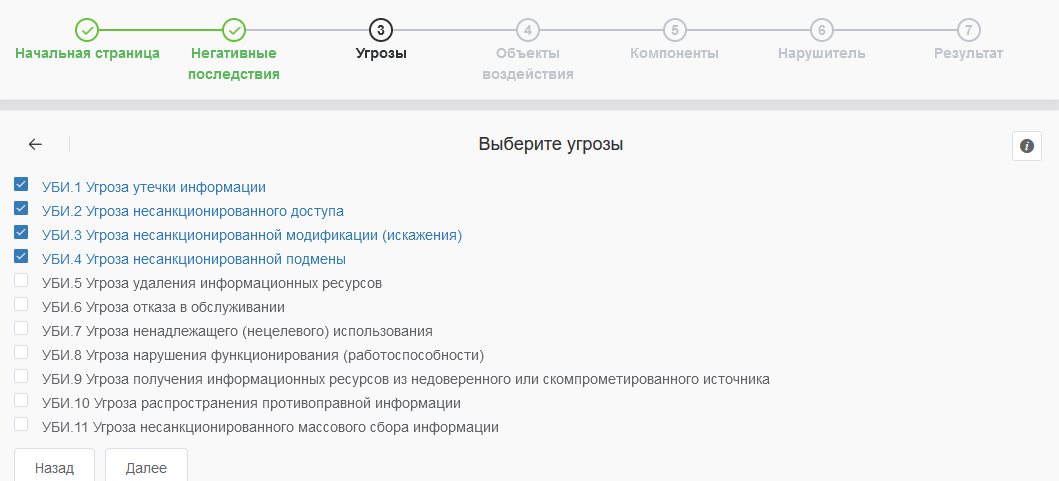


Рис. 14 – Угрозы определены автоматически

Далее выбираются объекты защиты, к которым автоматически будут выбраны компоненты, хотя снова есть возможность выбрать их самостоятельно.

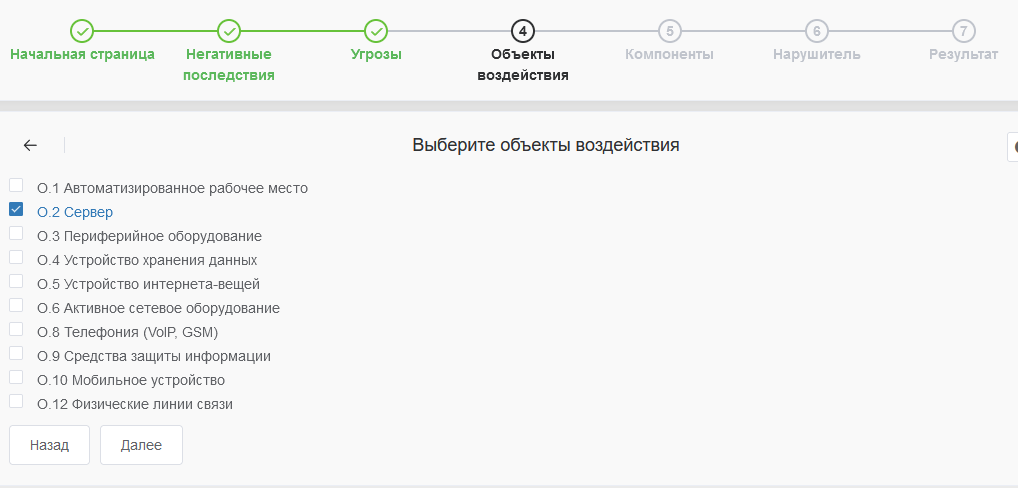


Рис. 15 – Выбор объектов воздействия

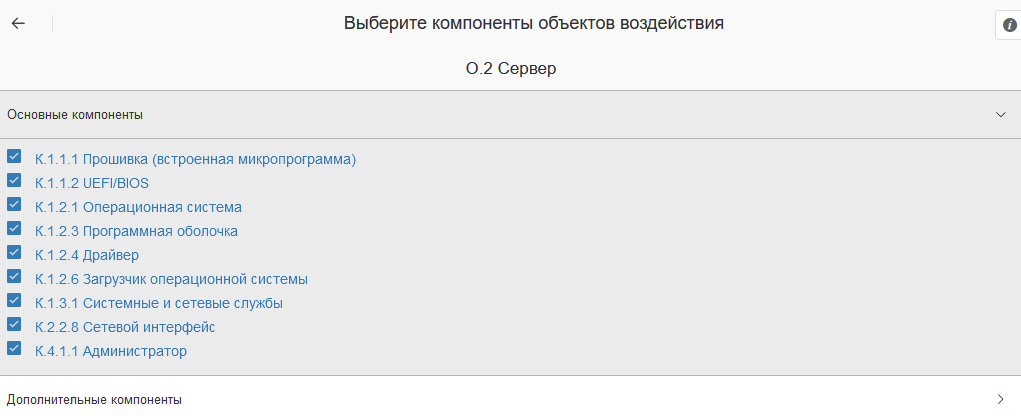


Рис. 16 – Компоненты объектов воздействия выбираются автоматически

Последним выбирается уровень нарушителя.

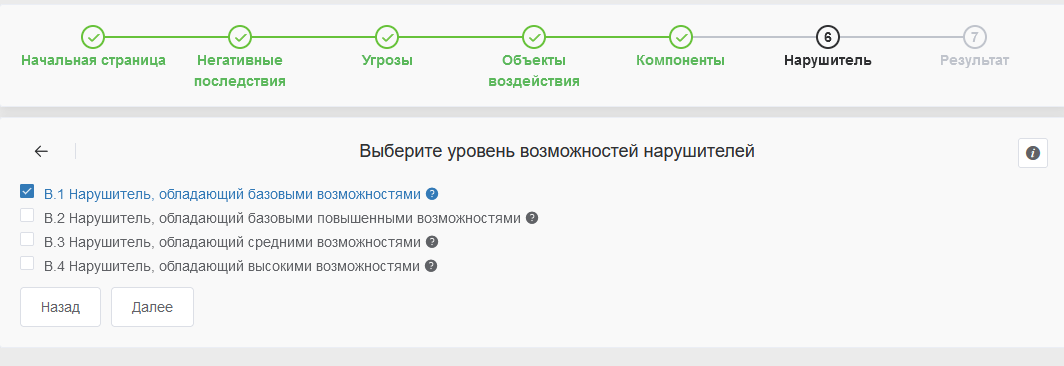


Рис. 17 – Выбор уровня нарушителя

В итоге получаем перечень угроз.

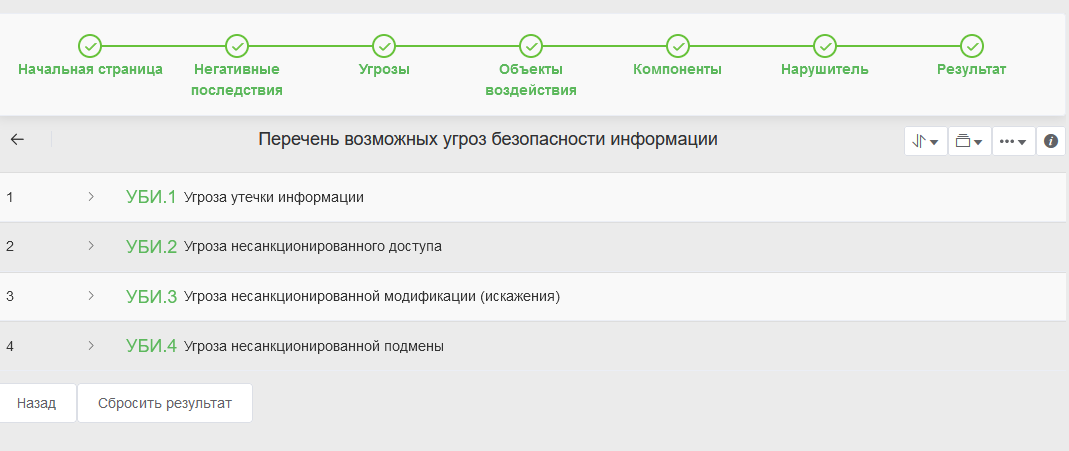


Рис. 18 – Перечень полученных угроз