МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доц., канд. техн. наук |  |  |  | В. М. Шишкин |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ |
| по курсу: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ |
|  |
|  |

РАБОТУ ВЫПОЛНИЛ(-А)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ(-КА) ГР. № | 3643 |  |  |  | Д.А.Дмитриева |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2018

Оглавление

[Введение 4](#_Toc511523576)

[Постановка задачи 5](#_Toc511523577)

[Объект защиты 5](#_Toc511523578)

[Проблема безопасности 5](#_Toc511523579)

[Цель безопасности 5](#_Toc511523580)

[Ограничения 5](#_Toc511523581)

[Компоненты объекта защиты 5](#_Toc511523582)

[Определение границ 5](#_Toc511523583)

[Спецификация окружения 5](#_Toc511523584)

[Источники угроз 6](#_Toc511523585)

[Угрозы 6](#_Toc511523586)

[События риска 6](#_Toc511523587)

[Компоненты объекта 6](#_Toc511523588)

[Граф взаимодействия источников угроз, событий риска и компонентов объект 7](#_Toc511523589)

[Матрица отношения W0 после арифметизации 7](#_Toc511523590)

[Транзитивная матрица V с профилем риска 8](#_Toc511523591)

[Анализ профиля риска 8](#_Toc511523592)

[Средства защиты информации 9](#_Toc511523593)

[Комплексы защиты информации 10](#_Toc511523594)

[Комплекс 1. Правовой 11](#_Toc511523595)

[Комплекс 2. Технический 11](#_Toc511523596)

[Комплекс 3. Смешанный 11](#_Toc511523597)

[Анализ отрицательных воздействий защиты информации 13](#_Toc511523598)

[Вывод 14](#_Toc511523599)

# Введение

Информационные системы- системы, предназначенные для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Информационная система предназначена для своевременного обеспечения надлежащих людей надлежащей информацией, то есть для удовлетворения конкретных информационных потребностей в рамках определенной предметной области, при этом результатом функционирования информационных систем является информационная продукция — документы, информационные массивы, базы данных и информационные услуги.

В настоящее время большая часть населения зарегистрирована в социальных сетях. Немалая часть людей пытаются взломать ту или иную страницу в социальной сети, или создать вирусы, которые сделали бы это.

Компьютерный вирус — вид вредоносного программного обеспечения, который способен создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение, а нарушение работы программно-аппаратных комплексов — удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей— часто является его сопутствующей функцией. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами.

# Постановка задачи

## Объект защиты

Рецепт антибиотика

## Проблема безопасности

Сохранение уникального рецепта антибиотика.

## Цель безопасности

## Компоненты объекта защиты

Бумажная версия рецепта, рецепт на жестком диске, руководящий производством состав

## Определение границ

Внешней границей является территория фабрики.

Внутренней границей является жесткий диск, документ, сотрудники-носители информации.

## Спецификация окружения

## Источники угроз

Уполномоченные сотрудники

Неуполномоченные сотрудники

Разработчик жесткого диска

Охранная организация

Постороннее лицо

## Угрозы

Некомпетентность сотрудника охраны

Кража ключа

Доступ в помещение

Установка скрытой аппаратуры злоумышленников

Намеренный вывод из строя систем безопасности и технических систем

Кража документа

Копирование документа

Несанкционированный доступ к информации

Санкционированный доступ к информации

Кража жесткого диска

Копирование данных с жесткого диска

Некомпетентность сотрудника разработки препарата

Запись разговора о создании и рецептуре препарата

Подслушана информация о рецепте в разговоре

Информацию о рецепте подглядели и запомнили

Кража данных с компьютера

Копирование данных с компьютера

Внедрение вредоносного ПО

Удаленный доступ к серверу

Доступ к серверу

Проникновение в серверную

## События риска

скопирована информация

украдена информация

информацию подслушали или подглядели

## Компоненты объекта

Документ

Жесткий диск

Компьютер

Сотрудник-носитель информации

Сотрудники вне производства

|  |
| --- |
|  |
| Рис.1.1 - Граф взаимодействия источников угроз, событий риска и компонентов объекта. |

## Матрица отношения W0 после арифметизации

|  |
| --- |
|  |
| Рис. 1.2 Матрица отношений |

## Транзитивная матрица V с профилем риска

|  |
| --- |
|  |
| Рис. X - Название рисунка |

# Анализ профиля риска

Бла бла бла профиль риска. Посмотрим на источники угроз.

|  |
| --- |
|  |
| Рис. X - Название рисунка |

Источник 1 явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен явно силен, но источник 2 тоже надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать надо учитывать.

Теперь угрозы

|  |
| --- |
|  |
| Рис. X - Название рисунка |

Угроза 1, 3, 4 больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность больше влияют на общую безопасность, надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать надо что-то делать, но не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5 не забывать и про угрозы 2, 5.

# Средства защиты информации

Средство 1 – это Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1 Средство 1

Средство 2 - Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2 Средство 2

Средство 3 - Средство 3 Средство 3 Средство 3 Средство 3 Средство 3 Средство 3 Средство 3 Средство 3

Средство 4 - Средство 4 Средство 4 Средство 4 Средство 4 Средство 4 Средство 4 Средство 4 Средство 4 Средство 4 Средство 4

Средство 5 - Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5 Средство 5

Средство 6 - Средство 6 Средство 6 Средство 6 Средство 6 Средство 6 Средство 6 Средство 6 Средство 6 Средство 6 Средство 6

Средство 7 - Средство 7 Средство 7 Средство 7 Средство 7 Средство 7 Средство 7 Средство 7 Средство 7.

Получаем таблицу

Таблица № – Название таблицы

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Источник 1 | Источник 2 | Угроза 1 | Угроза 2 | Угроза 3 | Угроза 4 | Угроза 5 | К-нт 1 | К-нт 2 | К-нт т 3 | Стоимость |
| Средство 1 | 0,1 | 0,5 | 0 | 0 | 0,2 | -0,2 | 0 | 0 | 0 | 0,1 | 10 |
| Средство 2 | 0 | 0 | 0,2 | 0,1 | 0,2 | 0 | 0,2 | 0 | 0,1 | 0 | 20 |
| Средство 3 | 0,2 | 0,2 | 0 | 0,2 | -0,2 | 0 | -0,3 | 0,1 | 0 | 0 | 30 |
| Средство 4 | 0 | 0,4 | 0,2 | 0 | 0,3 | 0,1 | 0 | 0,1 | 0 | 0 | 15 |
| Средство 5 | 0 | 0 | 0,2 | 0 | 0,2 | 0,2 | 0 | 0 | 0,1 | 0 | 25 |
| Средство 6 | 0,2 | 0 | 0,2 | 0,5 | 0 | 0,2 | 0 | 0 | 0 | 0,1 | 35 |
| Средство 7 | 0,4 | 0,4 | 0,2 | -0,2 | -0,1 | 0 | 0,2 | 0 | 0,1 | 0 | 5 |

## Комплексы защиты информации

Комплекс 1. Правовой – средство 1, 3, 4, общая стоимость 55.

Комплекс 2. Технический – средство 2, 5, 7, общая стоимость 50.

Комплекс 3. Смешанный – средство 1, 5, 6, общая стоимость 70.

## Комплекс 1. Правовой

|  |
| --- |
|  |
| Рис. X – Вектор r комплекса 1 |
|  |
| Рис. X – Матрица V с значением Rz |

Рассчитаем эффективность ez:

## Комплекс 2. Технический

|  |
| --- |
| Картинка вектора r |
| Рис. X – Вектор r комплекса 1 |
| Картинка матрицы V |
| Рис. X – Матрица V с значением Rz |

Рассчитаем эффективность ez:

## Комплекс 3. Смешанный

|  |
| --- |
| Картинка вектора r |
| Рис. X – Вектор r комплекса 1 |
| Картинка матрицы V |
| Рис. X – Матрица V с значением Rz |

Рассчитаем эффективность ez:

Выводы по расчетам.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Комплекс 1 | Комплекс 2 | Комплекс 3 |
| Rz | 0,6680 | 0,7680 | 0,7740 |
| cz | 55,0000 | 50,0000 | 70,0000 |
| ez | 0,0121 | 0,0154 | 0,0111 |

Из таблицы видно, что более эффективный 2 комплекс, лучшую оценку влияния (Rz) имеет третий комплекс, но он самый дорогой. Комплекс 1 показал меньшее значение Rz, но имеет преимущество перед самым дорогим. (Примерно так описываете результат, но конечно подумайте почему так получилось).

# Анализ отрицательных воздействий защиты информации

Описываете то, что может произойти при внедрении каких-то средств защиты. Например, усложнили политику паролей – пользователи перестали их запоминать – начали писать на бумажке – эту бумажку подсмотрел сотрудник другого отдела и передал информацию Вывод: необходимо еще потратить время на обучение сотрудников.

Или перешли на биометрическую пропускную систему – начали собирать больше информации о сотрудниках – охранная организация расторгла контракт, и охранник слил базу себе на флэшку. Вывод: надо еще потратить деньги и время, чтобы грамотно настроить доступ к БД системы контроля и управления доступом.

# Вывод

В выводе пишите, что у вас получилось, что вы узнали, каких результатов достигли, кому и в какой сфере деятельности может пригодиться ваша работа. Примерный объем не более страницы