

Действителен: с 28.05.2026 по 28.08.2027

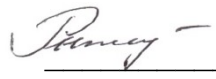
8.207 «Российский новый университет»

Елец  
2026 год

Одобрена  
предметной (цикловой)  
комиссией общеобразовательных  
дисциплин

Разработана на основе Федерального  
Государственного Образовательного  
Стандарта Среднего  
Профессионального Образования/  
ФГОС СПО/ по специальности 09.02.12  
Техническая эксплуатация и  
сопровождение информационных  
систем, утвержденного приказом  
Министерства просвещения РФ от  
10.03.2025 г. N 184

Протокол № 5  
от «28» 01 2026 г.  
Председатель предметной  
(цикловой) комиссии  
 / С.В. Толоконников

Начальник отделения СПО  
 / О.В. Рыжкова

Составитель (автор):  / пр. С.В. Толоконников

Рецензент: Суздальская Ева Анатольевна, заместитель начальника отдела  
эксплуатации средств вычислительной техники, программного  
обеспечения и телекоммуникационного оборудования управления  
информационных технологий – Отделение Социального фонда Российской  
Федерации по Липецкой области, г. Елец

## **1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

Программа учебной дисциплины Основы информационной безопасности предназначена для изучения информационной безопасности в профессиональных образовательных организациях, реализующих образовательную программу среднего общего образования в пределах освоения образовательной программы СПО на базе основного общего образования.

Программа разработана на основе Федерального Государственного Образовательного Стандарта Среднего Профессионального Образования/ ФГОС СПО/ по специальности 09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ (приказ Минобрнауки России от 10.03.2025 г. № 184).

Учебная дисциплина Основы информационной безопасности является учебным предметом обязательной предметной области «Естественно-научные предметы» ФГОС среднего общего образования. Учебная дисциплина Основы информационной безопасности изучается в общепрофессиональном цикле учебного плана ОП на базе основного общего образования с получением среднего общего образования. В учебных планах учебная дисциплина Основы информационной безопасности входит в состав профессиональных учебных дисциплин ФГОС среднего общего образования.

Целью изучения дисциплины: является формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях.

Главной задачей изучения теоретического курса для обучающихся является формирование представления о роли и месте знаний по дисциплине «Основы информационной безопасности» при освоении смежных дисциплин по выбранной специальности и в сфере профессиональной деятельности.

Развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств обеспечивается чтением лекций, проведением занятий с применением активных методов обучения, содержание которых разработано на основе результатов научных исследований, проводимых Университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей.

## **2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

В результате освоения дисциплины обучающийся по программе СПО по специальности должен:

*- Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам; (ОК 01.)*

**Знать:**

- источники угроз безопасности информации и меры по их предотвращению;
- сущность и понятие информационной безопасности, характеристику ее составляющих;
- виды, источники и носители защищаемой информации.

**Уметь:**

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- выявлять угрозы конфиденциальности, целостности, доступности информации;
- проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности.

***- Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности; (ОК 02.)***

**Знать:**

- место информационной безопасности в системе национальной безопасности страны;
- методы обработки, хранения, передачи и накопления информации; защиты информации от несанкционированного доступа; специализированным программным обеспечением для сбора, хранения и обработки информации;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах.

**Уметь:**

- классифицировать основные угрозы безопасности информации;
- разрабатывать документы организационно-распорядительного характера, регламентирующие работу по обеспечению информационной безопасности;
- использовать методы и средства защиты информации.

**3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С  
УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ,  
ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С  
ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА  
САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ**

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 час.).

| Вид учебной работы                            | Объем часов |
|-----------------------------------------------|-------------|
| <b>Максимальная учебная нагрузка (всего):</b> | <b>72</b>   |

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Обязательная аудиторная учебная нагрузка (всего)</b> | <b>52</b> |
| в том числе:                                            |           |
| Лекционные занятия (Лек)                                | 34        |
| Практические занятия (Пр)                               | 16        |
| Зачет с оценкой (З)                                     | 0,3       |
| Текущие консультации (ТКонс)                            | 1,7       |
| <b>Самостоятельная работа обучающегося (всего)</b>      | <b>20</b> |
| <b>Внеаудиторная самостоятельная работа</b>             |           |

**Распределение учебного времени по темам и видам учебных занятий  
очная форма обучения**

| №                                  | Наименование разделов, тем учебных занятий                       | Всего часов | Контактная работа с преподавателем |     |    |   |      |     |       | Сам. раб | Формируемые результаты обучения |
|------------------------------------|------------------------------------------------------------------|-------------|------------------------------------|-----|----|---|------|-----|-------|----------|---------------------------------|
|                                    |                                                                  |             | Всего                              | Лек | Пр | З | Конс | КоР | ТКонс |          |                                 |
| Основы информационной безопасности |                                                                  |             |                                    |     |    |   |      |     |       |          |                                 |
| 1                                  | Основные понятия и задачи информационной безопасности            | 8           | 6                                  | 6   |    |   |      |     |       | 2        | ОК 01,<br>ОК 02                 |
| 2                                  | Нормативно-правовое регулирование защиты информации              | 12          | 10                                 | 8   | 2  |   |      |     |       | 2        |                                 |
| 3                                  | Классификация безопасности                                       | 10          | 6                                  | 4   | 2  |   |      |     |       | 4        |                                 |
| 4                                  | Документооборот, как способ защиты информации                    | 12          | 8                                  | 4   | 4  |   |      |     |       | 4        |                                 |
| 5                                  | Угрозы безопасности защиты информации и основы защиты информации | 16          | 12                                 | 8   | 4  |   |      |     |       | 4        |                                 |
| 6                                  | Методологические подходы к защите информации                     | 12          | 8                                  | 4   | 4  |   |      |     |       | 4        |                                 |

|   |                                            |   |   |  |  |     |  |  |     |  |  |
|---|--------------------------------------------|---|---|--|--|-----|--|--|-----|--|--|
| 7 | Промежуточная аттестация (зачет с оценкой) | 2 | 2 |  |  | 0,3 |  |  | 1,7 |  |  |
|---|--------------------------------------------|---|---|--|--|-----|--|--|-----|--|--|

#### **4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ)**

##### Тема 1. Основные понятия и задачи информационной безопасности

Введение в дисциплину. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятия компонента, класса и семейства. Объективно-ориентированный подход к информационной безопасности.

##### Тема 2. Нормативно-правовое регулирование защиты информации

Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности. Информационная безопасность распределенных систем. Администрирование средств безопасности. Стандарты и спецификации в области информационной безопасности. Определение объектов защиты на типовом объекте информатизации

##### Тема 3. Классификация безопасности

Основные понятия и механизмы информационной безопасности. Классы безопасности. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. Определение угроз объекта информатизации и их классификация

##### Тема 4. Документооборот, как способ защиты информации

Правила и порядок оформления документов. Документооборот и его организация.

##### Тема 5. Угрозы безопасности защиты информации и основы защиты информации

Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Угрозы информационной безопасности Способы защиты информации. Аппаратные и программные средства обеспечения безопасности государства. Защита от информационных утечек Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи. Защита информации, содержащей коммерческую, государственную и иные виды тайн. Антивирусные программ и их использование. Работа в справочно-правовой

системе с нормативными и правовыми документами по информационной безопасности.

## **Тема 6. Методологические подходы к защите информации**

Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы. Выбор мер защиты информации для автоматизированного рабочего места.

## **Тема 7. Промежуточная аттестация (зачет с оценкой)**

Решение конкретной теоретической или практической задачи для установления степени усвоения изучаемого материала студентом.

См. приложение 1 «Вопросы к зачету с оценкой»

## **Планы практических занятий**

**Тема 2. Нормативно-правовое регулирование защиты информации.**

Время - 2 час.

Основные вопросы: Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности. Информационная безопасность распределенных систем. Администрирование средств безопасности. Стандарты и спецификации в области информационной безопасности. Определение объектов защиты на типовом объекте информатизации.

См. Приложение 2 «Практические работы».

**Тема 3. Классификация безопасности.**

Время - 2 час.

Основные вопросы: Основные понятия и механизмы информационной безопасности. Классы безопасности. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. Определение угроз объекта информатизации и их классификация

См. Приложение 2 «Практические работы».

**Тема 4. Документооборот, как способ защиты информации.**

Время - 4 час.

Основные вопросы: Правила и порядок оформления документов. Документооборот и его организация.

См. Приложение 2 «Практические работы».

**Тема 5. Угрозы безопасности защиты информации и основы защиты информации.**

Время - 4 час.

Основные вопросы: Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Угрозы информационной безопасности Способы защиты информации. Аппаратные и программные средства обеспечения безопасности государства. Защита от информационных утечек Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи. Защита информации, содержащей коммерческую, государственную и иные виды тайн. Антивирусные программ и их использование. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

См. Приложение 2 «Практические работы».

Тема 6. Методологические подходы к защите информации.

Время - 4 час.

Основные вопросы: Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы. Выбор мер защиты информации для автоматизированного рабочего места.

См. Приложение 2 «Практические работы».

## **5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

### **5.1.1. Методические указания:**

Самостоятельная работа обучающихся, это работа, выполняемая во внеаудиторное (аудиторное) время при методическом руководстве преподавателя с целью овладения необходимыми компетенциями по дисциплине, дополнительными знаниями, умениями и навыками, опытом творческой, исследовательской деятельности, развития самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного уровня.

Видами заданий для самостоятельной работы являются:

1. Заполнение глоссария
2. Поиск и анализ источников и литературы
3. Подготовка сообщений, презентаций, докладов, рефератов
4. Выполнение практических работ
5. Решение задач

Для выполнения заданий по самостоятельной работе рекомендуется использовать материалы учебников и интернет ресурсов:

### Основная литература:

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588374>
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587457>
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587458>

### Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588246>
2. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584372>
3. Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Профессиональное образование). — ISBN 978-5-534-20505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590434>
4. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Профессиональное образование). — ISBN 978-5-534-20645-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590435>

5. Осокин, А. Н. Теория информации : учебник для среднего профессионального образования / А. Н. Осокин, А. Н. Мальчуков. — Москва : Издательство Юрайт, 2025. — 208 с. — (Профессиональное образование). — ISBN 978-5-534-17296-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566418>

### **Интернет-ресурсы:**

<https://securelist.ru/enciklopediya> - Энциклопедия информационной безопасности.

<http://www.citforum.ru/security/> - CITFORUM — информационная безопасность (большое количество материалов по теме).

<http://www.comp-doctor.ru/> - Компьютер и здоровье: болезни от компьютера, профилактика и лечение.

<http://www.microsoft.com/rus/protect/default.aspx#> Вопросы обеспечения информационной безопасности от компании Microsoft

<http://www.saferinternet.ru/> - Безопасный интернет - специальный портал, созданный по вопросам безопасного использования сети Интернет

<http://www.infoforum.ru/> - Национальный форум информационной безопасности "ИНФОФОРУМ"

<http://mon.gov.ru/> (Сайт Министерства образования и науки РФ) /

[www.edu.ru](http://www.edu.ru) (Российский образовательный портал).

[www.ed.gov.ru](http://www.ed.gov.ru) (Сайт Федерального агентства по образованию РФ).

<http://elibrary.rsl.ru/> Российская государственная публичная библиотека

<http://www.rambler.ru> – Русская поисковая система.

<http://www.yandex.ru> – Русская поисковая система.

<http://biblioteka.net.ru> – Библиотека компьютерных учебников.

Портал «Всеобуч»- справочно-информационный образовательный сайт, единое окно доступа к образовательным ресурсам –<http://www.edu-all.ru/>

### **Рекомендации по составлению и заполнению глоссария:**

Использование глоссария способствует прояснению, запоминанию и уточнению ключевых понятий дисциплины. Глоссарий охватывает все узкоспециализированные термины, встречающиеся в тексте. Глоссарий должен содержать не менее 30 терминов, они должны быть перечислены в алфавитном порядке, соблюдена нумерация. Глоссарий должен быть оформлен по принципу реферативной работы, в обязательном порядке присутствует титульный лист и нумерация страниц. Объем работы должен составлять 10-15 страниц. Тщательно проработанный глоссарий помогает избежать разночтений и улучшить в целом качество всей документации. В глоссарии включаются самые частотные термины и фразы, а также все ключевые термины с толкованием их смысла. Глоссарии могут содержать отдельные слова, фразы, аббревиатуры, слоганы и даже целые предложения.

### **Рекомендации по поиску и анализу источников и литературы**

Найдите дополнительные источники литературы и источники, максимально соответствующие теме (заданию) и рекомендованные преподавателем. Ознакомьтесь с аннотацией источника, ее содержанием по оглавлению. Найдите необходимый материал и просмотрите его содержание. Определите форму записи (конспект, тезисы, цитаты, выписки, факты), составьте план и обсудите с преподавателем. Выпишите незнакомые слова и найдите их определение в словаре или спросите у преподавателя. Выполните краткий конспект. В конце своих записей сделайте резюме к тексту.

Рекомендации по подготовке сообщений, презентаций, докладов, рефератов

Внимательно прочитайте тему доклада, составьте предполагаемый план раскрытия темы, обсудите его с преподавателем. При работе с источниками информации тщательно отбирайте примеры, факты, следите за логикой их обоснования. Помните, что объем вашего выступления не должен выходить за предложенные преподавателем нормы. Выберите из подготовленного текста наиболее существенные моменты будущего выступления и согласуйте с преподавателем. При необходимости сопроводите свое выступление иллюстрациями или подготовьте презентацию. Презентация должна быть краткой, доступной и целостной. Главное в презентации – содержание. Придерживайтесь единого стилевого оформления. Не рекомендуется использовать в стилевом оформлении презентации более трех цветов или трех типов шрифта. Оформление слайда не должно отвлекать от его содержательной части. Не все слайды презентации должны быть выдержаны в одном стиле.

На одном слайде не должно быть слишком много информационных блоков, обычно до трёх. Ключевые слова в информационном блоке необходимо выделить. Наиболее важную информацию – поместить в центр слайда. Приводите факты, цифры, графики - это хорошая поддержка для вашего выступления. Голый текст никого не интересует (если вы, конечно, не несете слушателям свет новой истины). Применяйте высококонтрастные цвета, крупные шрифты и четкие иллюстрации. Фотографии, рисунки и другие иллюстрации старайтесь размещать на отдельных слайдах. То же относится большим диаграммам, таблицам, схемам и графикам. Не забывайте указывать источники информации.

Приступая к подготовке реферата, доклада, на первом этапе, нужно собрать информацию. Можно использовать книги, статьи, научные публикации и интернет-ресурсы. Во время исследования нужно делать заметки, выделяя ключевые моменты, факты и примеры. Доклад необходимо структурировать. Обычно он включает три раздела: Введение - представить тему и объяснить её актуальность. Основная часть - разделить на несколько логически связанных частей. Каждая часть должна содержать ключевые идеи и факты. Заключение -

подвести итоги, сделать выводы, дать рекомендации или предложить направления для дальнейшего изучения темы.

Подготовить визуальные материалы. Если доклад предполагает наличие презентации, нужно создать слайды, которые помогут визуализировать информацию.

Рекомендации по выполнению практических работ

Ознакомьтесь с темой, целью и заданием практической работы. Повторите теоретический материал, необходимый для выполнения работы.

Пройдите инструктаж по технике безопасности, если работа связана с оборудованием или лабораторными условиями. Запишите дату, тему и цель работы.

Следуйте предложенному алгоритму действий, если он есть. Работайте аккуратно, используйте линейки, карандаши, разборчивый почерк. Таблицы и схемы оформляйте чётко и по правилам.

По итогам работы сформулируйте выводы, ответьте на контрольные вопросы.

Проверьте, чтобы все расчёты и ответы были выполнены полностью и правильно.

Если работа письменная, составьте план, продумайте логику изложения, аргументируйте свои решения.

При возникновении трудностей обращайтесь к преподавателю или дополнительной литературе.

Соблюдайте требования к оформлению: аккуратность, читаемость, соответствие стандартам.

Рекомендации по самостоятельному изучению:

Начните с базовых понятий каждой категории

Решайте практические задачи регулярно

Используйте несколько источников для лучшего понимания

Создавайте конспекты и схемы

Применяйте изученное на практике

Участвуйте в онлайн-форумах и обсуждениях

Проверяйте свои знания через тесты и контрольные работы

Дополнительные советы:

Регулярность - занимайтесь минимум 30 минут ежедневно

Системность - следуйте логической последовательности изучения

Практика - решайте как можно больше задач

Обратная связь - проверяйте решения и исправляйте ошибки

Мотивация - ставьте конкретные цели и отслеживайте прогресс

Задания по самостоятельной работе должны быть выполнены до начала промежуточной аттестации.

Критерии оценки защиты мультимедийной презентации:

Оценка 5 ставится, если выполнены все требования к созданию мультимедийной презентации: обозначена тема, выполнен краткий анализ различных источников по данной теме, сформулированы выводы, выдержан объём, соблюдены требования к оформлению: фон, шрифт, объём текста, рисунки, анимация, выдержан единый стиль оформления

Оценка 4 – основные требования созданию мультимедийной презентации и ее защите выполнены, но при этом допущены недочёты: имеются неточности в изложении материала; отсутствует логическая последовательность; не выдержан объём презентации; имеются упущения в оформлении: не полностью соблюден единый стиль оформления.

Оценка 3 – имеются существенные отступления от требований к созданию мультимедийной презентации: не полностью раскрыта тема, имеются существенные недочёты в оформлении.

Оценка 2 – тема презентации не раскрыта, не соблюден единый стиль оформления слайдов.

Критерии оценки выступления с сообщением:

Оценка 5 - выполнены все требования к написанию и защите сообщения: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка 4 – основные требования к сообщению и их защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка 3 – имеются существенные отступления от требований: тема освещена лишь частично; допущены фактические ошибки в содержании или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

Оценка 2 – тема не раскрыта, обнаруживается существенное непонимание проблемы.

Критерии оценки устных ответов:

Оценка 5 – обучающийся полно излагает изученный материал, дает правильное определение языковых понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно

составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.

Оценка 4 – обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочета в последовательности и языковом оформлении излагаемого.

Оценка 3 – обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий и формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.

Оценка 2 – обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «2» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

#### 5.1.2. Задания для повторения и углубления приобретаемых знаний.

| №  | Задания                                                                            |
|----|------------------------------------------------------------------------------------|
| 1  | Понятие политики безопасности.                                                     |
| 2  | Понятие угрозы безопасности информации                                             |
| 3  | Уязвимости. Методы оценки уязвимости информации                                    |
| 4  | Анализ существующих методик определения требований к защите информации             |
| 5  | Организационная структура системы защиты информации                                |
| 6  | Законодательные акты в области защиты информации                                   |
| 7  | Основные правила системы сертификации РФ в области защиты информации               |
| 8  | Основные документы системы сертификации РФ в области защиты информации             |
| 9  | Меры защиты информации, реализуемые в автоматизированных (информационных) системах |
| 10 | Организационно-распорядительная защита информации                                  |

#### 1.2. Задания, направленные на формирование профессиональных умений.

| № | Задания |
|---|---------|
|---|---------|

|    |                                                                                                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11 | Системная классификация угроз безопасности информации                                                                                                                |
| 12 | Каналы несанкционированного доступа к информации                                                                                                                     |
| 13 | Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.                                                                  |
| 14 | Виды мер и основные принципы защиты информации.                                                                                                                      |
| 15 | Российские и международные стандарты, определяющие требования к защите информации                                                                                    |
| 16 | Система сертификации РФ в области защиты информации                                                                                                                  |
| 17 | Основные механизмы защиты информации                                                                                                                                 |
| 18 | Система защиты информации.                                                                                                                                           |
| 19 | Инженерная защита объектов информатизации                                                                                                                            |
| 20 | Классификация угроз информационной безопасности РФ по общей направленности. 48. Основные положения ФЗ «Об информации, информационных технологиях и защите информации |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

### 6.1. Средства оценивания в ходе текущего контроля:

#### Перечень знаний, осваиваемых в рамках учебной дисциплины

| Результаты обучения                                                                                                                                                                                                                                                                                                                                                       | Критерии оценки                                                                                                                                                                                                                                             | Методы оценки                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- источники угроз безопасности информации и меры по их предотвращению;</li> <li>- сущность и понятие информационной безопасности, характеристику ее составляющих;</li> <li>- виды, источники и носители защищаемой информации.</li> <li>- классифицировать защищаемую информацию по видам тайны и степеням секретности;</li> </ul> | <ul style="list-style-type: none"> <li>- знание и понимание материала;</li> <li>- грамотное использование терминологии в ходе устных и письменных ответов;</li> <li>- критическое мышление и решение проблем;</li> <li>- коммуникативные навыки;</li> </ul> | <ul style="list-style-type: none"> <li>- устные опросы в ходе аудиторных занятий на знание категорий дисциплины;</li> <li>- письменные опросы в ходе аудиторных занятий на знание категорий дисциплины;</li> <li>- сообщения или доклады в ходе практических занятий;</li> <li>- выполнение заданий в ходе практических занятий;</li> </ul> |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- выявлять угрозы конфиденциальности, целостности, доступности информации;</li> <li>- проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>- выполнение заданий и упражнений, рекомендованных для самостоятельной работы;</li> <li>- зачет с оценкой</li> </ul>                                                                                                                                                                                                                                                                                                    |
| <ul style="list-style-type: none"> <li>- место информационной безопасности в системе национальной безопасности страны;</li> <li>- методы обработки, хранения, передачи и накопления информации; защиты информации от несанкционированного доступа; специализированным программным обеспечением для сбора, хранения и обработки информации;</li> <li>- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах.</li> <li>- классифицировать основные угрозы безопасности информации;</li> <li>- разрабатывать документы организационно-распорядительного характера, регламентирующие работу по обеспечению информационной безопасности;</li> <li>- использовать</li> </ul> | <ul style="list-style-type: none"> <li>- знание и понимание материала;</li> <li>- грамотное использование терминологии в ходе устных и письменных ответов;</li> <li>- критическое мышление и решение проблем;</li> <li>- коммуникативные навыки;</li> </ul> | <ul style="list-style-type: none"> <li>- устные опросы в ходе аудиторных занятий на знание категорий дисциплины;</li> <li>- письменные опросы в ходе аудиторных занятий на знание категорий дисциплины;</li> <li>- сообщения или доклады в ходе практических занятий;</li> <li>- выполнение заданий в ходе практических занятий:</li> <li>- выполнение заданий и упражнений, рекомендованных для самостоятельной работы;</li> <li>- зачет с оценкой</li> </ul> |

|                                     |  |  |
|-------------------------------------|--|--|
| методы и средства защиты информации |  |  |
|-------------------------------------|--|--|

## 6.2. ФОС для текущего контроля:

См. Приложение 3 «ФОС для текущего контроля»

## 6.3 ФОС для промежуточной аттестации:

Задания для оценки знаний.

| № | Задания                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Вопросы к зачету с оценкой 1-8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2 | <ol style="list-style-type: none"> <li>1. Введение в дисциплину. Понятие информации и информационной безопасности.</li> <li>2. Информация, сообщения, информационные процессы как объекты информационной безопасности.</li> <li>3. Обзор защищаемых объектов и систем.</li> <li>4. Понятия компонента, класса и семейства.</li> <li>5. Объективно-ориентированный подход к информационной безопасности.</li> <li>6. Российское законодательство в области информационной безопасности.</li> <li>7. Зарубежное законодательство в области информационной безопасности.</li> <li>8. Информационная безопасность распределенных систем</li> </ol> |
| 3 | Вопросы к зачету с оценкой 9-16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 4 | <ol style="list-style-type: none"> <li>9. Администрирование средств безопасности.</li> <li>10. Стандарты и спецификации в области информационной безопасности.</li> <li>11. Определение объектов защиты на типовом объекте информатизации</li> <li>12. Основные понятия и механизмы информационной безопасности. Классы безопасности.</li> <li>13. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.</li> <li>14. Определение угроз объекта информатизации и их классификация</li> <li>15. Правила и порядок оформления документов.</li> <li>16. Документооборот и его организация</li> </ol>                  |
| 5 | Вопросы к зачету с оценкой 17-25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 6 | <ol style="list-style-type: none"> <li>17. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.</li> <li>18. Угрозы информационной безопасности</li> <li>19. Способы защиты информации.</li> <li>20. Аппаратные и программные средства обеспечения</li> </ol>                                                                                                                                                                                                                                                                                                                                   |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | безопасности государства.<br>21. Защита от информационных утечек<br>22. Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи.<br>23. Защита информации, содержащей коммерческую, государственную и иные виды тайн.<br>24. Антивирусные программ и их использование.<br>25. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности                                               |
| 7 | Вопросы к зачету с оценкой 26-32                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 8 | 26. Анализ существующих методик определения требований к защите информации.<br>27. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.<br>28. Виды мер и основные принципы защиты информации.<br>29. Организационно-распорядительная защита информации.<br>30. Работа с кадрами и внутриобъектовый режим.<br>31. Принципы построения организационно-распорядительной системы.<br>32. Выбор мер защиты информации для автоматизированного рабочего места |

Задания для оценки умений.

См. Приложение 4 «Задания для самостоятельной работы»

## 7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная литература:

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588374>
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587457>
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования /

А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587458>

#### Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588246>

2. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584372>

3. Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Профессиональное образование). — ISBN 978-5-534-20505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590434>

4. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Профессиональное образование). — ISBN 978-5-534-20645-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590435>

5. Осокин, А. Н. Теория информации : учебник для среднего профессионального образования / А. Н. Осокин, А. Н. Мальчуков. — Москва : Издательство Юрайт, 2025. — 208 с. — (Профессиональное образование). — ISBN 978-5-534-17296-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566418>

#### Интернет-ресурсы:

<https://urait.ru> Образовательная платформа Юрайт. Для вузов и ссузов  
<https://securelist.ru/enciklopediya> - Энциклопедия информационной безопасности.

<http://www.citforum.ru/security/> - CITFORUM — информационная безопасность (большое количество материалов по теме).

<http://www.comp-doctor.ru/> - Компьютер и здоровье: болезни от компьютера, профилактика и лечение.

<http://www.microsoft.com/rus/protect/default.aspx#> Вопросы обеспечения информационной безопасности от компании Microsoft

<http://www.saferinternet.ru/> - Безопасный интернет - специальный портал, созданный по вопросам безопасного использования сети Интернет

<http://www.infoforum.ru/> - Национальный форум информационной безопасности "ИНФОФОРУМ"

<http://mon.gov.ru/> (Сайт Министерства образования и науки РФ) / [www.edu.ru](http://www.edu.ru) (Российский образовательный портал).

[www.ed.gov.ru](http://www.ed.gov.ru) (Сайт Федерального агентства по образованию РФ).

<http://elibrary.rsl.ru/> Российская государственная публичная библиотека

<http://www.rambler.ru> – Русская поисковая система.

<http://www.yandex.ru> – Русская поисковая система.

<http://biblioteka.net.ru> – Библиотека компьютерных учебников.

Портал «Всеобуч»- справочно-информационный образовательный сайт, единое окно доступа к образовательным ресурсам –<http://www.edu-all.ru/>

## **8. ПЕРЕЧЕНЬ КОМПЛЕКТОВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

При изучении учебной дисциплины (в том числе в интерактивной форме) предполагается применение современных информационных технологий. Комплект программного обеспечения для их использования включает в себя: свободно распространяемое программное обеспечение OpenOffice; веб-браузер (Google Chrome); электронные библиотечные системы IPR Smart и ЮРАЙТ; систему размещения в сети «Интернет» и проверки на наличие заимствований курсовых, научных и выпускных квалификационных работ «Антиплагиат.ВУЗ».

Для доступа к учебному плану и результатам освоения дисциплины, формирования Портфолио обучающегося используется Личный кабинет студента (он-лайн доступ через сеть Интернет <https://portal.rosnou.ru>). Для обеспечения доступа обучающихся во внеучебное время к электронным образовательным ресурсам учебной дисциплины ЮРАЙТ и IPR Smart, а также для студентов, обучающихся с применением дистанционных образовательных технологий, используется портал через сеть Интернет <https://e-edu.rosnou.ru>, <https://id.rosnou.ru>.

## **9. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

<https://urait.ru> Образовательная платформа Юрайт. Для вузов и ссузов

<https://securelist.ru/enciklopediya> - Энциклопедия информационной безопасности.

<http://www.citforum.ru/security/> - CITFORUM — информационная безопасность (большое количество материалов по теме).

<http://www.comp-doctor.ru/> - Компьютер и здоровье: болезни от компьютера, профилактика и лечение.

<http://www.microsoft.com/rus/protect/default.aspx#> Вопросы обеспечения информационной безопасности от компании Microsoft

<http://www.saferinternet.ru/> - Безопасный интернет - специальный портал, созданный по вопросам безопасного использования сети Интернет

<http://www.infoforum.ru/> - Национальный форум информационной безопасности "ИНФОФОРУМ"

<http://mon.gov.ru/> (Сайт Министерства образования и науки РФ) / [www.edu.ru](http://www.edu.ru) (Российский образовательный портал).

[www.ed.gov.ru](http://www.ed.gov.ru) (Сайт Федерального агентства по образованию РФ).

<http://elibrary.rsl.ru/> Российская государственная публичная библиотека

<http://www.rambler.ru> – Русская поисковая система.

<http://www.yandex.ru> – Русская поисковая система.

<http://biblioteka.net.ru> – Библиотека компьютерных учебников.

Портал «Всеобуч»- справочно-информационный образовательный сайт, единое окно доступа к образовательным ресурсам –<http://www.edu-all.ru/>

## **10. ОБУЧЕНИЕ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

Изучение учебной дисциплины обучающимися инвалидами и лицами с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства просвещения РФ от 31 марта 2025 г. № 253 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере общего, среднего профессионального образования и соответствующего дополнительного профессионального образования, профессионального обучения, дополнительного образования детей и взрослых, организации отдыха и оздоровления детей, а также оказания им при этом необходимой помощи», Положением АНО ВО «РосНОУ» Об организации обучения студентов – инвалидов и лиц с ограниченными возможностями здоровья.

Лица с ограниченными возможностями здоровья и инвалиды обеспечиваются электронными образовательными ресурсами, адаптированными к состоянию их здоровья.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации на основании просьбы, выраженной в письменной форме.

С обучающимися по индивидуальному плану или индивидуальному графику проводятся индивидуальные занятия и консультации.

## **11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО**

## ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения лекционных занятий (поточная), оснащенная оборудованием: специализированная мебель; маркерная доска (переносная), проектор (портативный); экран (переносной); ноутбук для преподавателя (с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза); колонки; микрофон, наглядные пособия (плакаты).

Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, воспитательной работы (**Лаборатория Информатики и информационных компьютерных технологий в профессиональной деятельности**), оснащенная оборудованием: специализированная мебель; магнитно-маркерная доска; проектор; экран; телевизор; ПК для преподавателя или ноутбук (с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза), персональные компьютеры в сборке с пакетом специализированных программ; наглядные пособия (плакаты).

Помещение для самостоятельной работы обучающихся, оснащенное оборудованием: персональные компьютеры в сборке с пакетом специализированных программ, с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду.

Учебная аудитория для занятий обучающихся из числа инвалидов и лиц с ОВЗ. Специализированная мебель (стол для инвалидов-колясочников СИ-1), проектор; экран; мнемосхема тактильная; персональные компьютеры в сборке со специализированным пакетом программ, клавиатура с подсветкой с возможностью работы слабовидящим; комплект для маркировки Брайлем (клавиатура для компьютера); индукционная система переносная ИЦР-2.

**«Вопросы к зачету с оценкой»**

1. Введение в дисциплину. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятия компонента, класса и семейства.
5. Объективно-ориентированный подход к информационной безопасности.
6. Российское законодательство в области информационной безопасности.
7. Зарубежное законодательство в области информационной безопасности.
8. Информационная безопасность распределенных систем
9. Администрирование средств безопасности.
10. Стандарты и спецификации в области информационной безопасности.
11. Определение объектов защиты на типовом объекте информатизации
12. Основные понятия и механизмы информационной безопасности. Классы безопасности.
13. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.
14. Определение угроз объекта информатизации и их классификация
15. Правила и порядок оформления документов.
16. Документооборот и его организация
17. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
18. Угрозы информационной безопасности
19. Способы защиты информации.
20. Аппаратные и программные средства обеспечения безопасности государства.
21. Защита от информационных утечек
22. Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи.
23. Защита информации, содержащей коммерческую, государственную и иные виды тайн.
24. Антивирусные программ и их использование.
25. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности

26. Анализ существующих методик определения требований к защите информации.

27. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.

28. Виды мер и основные принципы защиты информации.

29. Организационно-распорядительная защита информации.

30. Работа с кадрами и внутриобъектовый режим.

31. Принципы построения организационно-распорядительной системы.

32. Выбор мер защиты информации для автоматизированного рабочего места

## Практические работы

### Практическая работа № 1 «Персональные данные как вид защищаемой информации»

**Задание 1.** С использованием любой правовой информационно-поисковой системы («Гарант», «Консультант Плюс» и др.), заполните следующую таблицу:

| Вопрос                                                                                                                                                                           | Ответ |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Основные понятия, используемые в законе.                                                                                                                                         |       |
| Каким законодательством регламентируются персональные данные.                                                                                                                    |       |
| Основные методы и принципы обработки персональных данных.                                                                                                                        |       |
| Для чего необходима защита персональных данных.                                                                                                                                  |       |
| В чем заключается конфиденциальность персональных данных.                                                                                                                        |       |
| Какие данные в соответствии с законом входят в разряд персональных.                                                                                                              |       |
| В каких случаях допускается обработка персональных данных специальных категорий.                                                                                                 |       |
| Что такое биометрические данные, как они обрабатываются.                                                                                                                         |       |
| Как передаются персональные данные на территории иностранных государств.                                                                                                         |       |
| Как обрабатываются персональные данные в Государственных органах, муниципальных органах.                                                                                         |       |
| На получение каких сведений имеет право субъект, в какой форме сведения должны быть предоставлены.                                                                               |       |
| Права субъектов персональных данных на основании автоматизированной их обработки. Кто такой оператор, его обязанности и что он обязан предоставить субъекту персональных данных. |       |
| Как представляется уведомление об обработке персональных данных.                                                                                                                 |       |
| Ответственные за организацию обработки персональных данных в организациях их обязанности и ответственность.                                                                      |       |
| Федеральный орган, отвечающий за защиту прав субъектов персональных данных.                                                                                                      |       |
| Требования к защите персональных данных. Ответственность за нарушение федерального закона ФЗ №152.                                                                               |       |

**Задание 2.** С использованием любой правовой информационно-поисковой системы («Гарант», «Консультант Плюс» и др.), заполните следующие таблицы:

| <b>Конституция РФ</b> |                |              |                   |                      |
|-----------------------|----------------|--------------|-------------------|----------------------|
| Номер главы           | Название главы | Номер статьи | Содержание статьи | Комментарии к статье |
|                       |                |              |                   |                      |

| <b>Доктрина информационной безопасности РФ</b> |               |                     |                          |
|------------------------------------------------|---------------|---------------------|--------------------------|
| Номер                                          | Дата принятия | Основное содержание | Примечания (при наличии) |
|                                                |               |                     |                          |

| <b>УК РФ Глава 28. Преступления в сфере компьютерной информации</b>                            |                            |                                                                            |                                        |                                          |                          |
|------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------|----------------------------------------|------------------------------------------|--------------------------|
| Номер статьи УК РФ                                                                             | Дата редакции статьи УК РФ | Название статьи УК РФ                                                      | Причина наказания                      | Какое наказание предусмотрено            | Примечания (при наличии) |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| Номер закона                                                                                   | Дата принятия              | Даты принятия и одобрения закона Государственной думой и советом Федерации | Основные понятия используемые в законе | Количество статей в законе и их названия | Информация об изменениях |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «Об информации, информационных технологиях и защите информации»</b>                      |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «О лицензировании отдельных видов деятельности»</b>                                      |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»</b> |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «О коммерческой тайне»</b>                                                               |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «Об электронной подписи»</b>                                                             |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «О персональных данных»</b>                                                              |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |
| <b>ФЗ «О государственной тайне»</b>                                                            |                            |                                                                            |                                        |                                          |                          |
|                                                                                                |                            |                                                                            |                                        |                                          |                          |

## **Практическая работа № 2. «Безопасность и защита информации».**

В соответствии с пунктом 1 статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и защите информации" (в ред. от 27.07.2010) защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации.

Говоря о защите информации в целом, прежде всего, следует различать требования, предъявляемые к защите сведений:

- составляющих государственную тайну;
- признаваемые коммерческой тайной;
- персонального характера.

Российское законодательство о защите персональных данных является относительно новым и существует множество нерешенных вопросов, что зачастую препятствует выполнению операторами персональных данных необходимых требований действующего законодательства о персональных данных. Однако, несмотря на значительный комплекс проблем необходимо понимать, что:

1. Все без исключения физические лица являются субъектами ПДн.
2. Все без исключения организации являются операторами персональных данных и должны рассматривать требования Закона о персональных данных с точки зрения обеспечения наших прав и свобод, закрепленных Конституцией РФ.
3. Четкое выполнение требований регуляторов (Роскомнадзор, ФСТЭК России, ФСБ России) - уменьшение рисков манипулирования со стороны персонала и конкурентов. Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн.

Для соблюдения минимальных требований и недопущения серьезных претензий со стороны регуляторов (в первую очередь Роскомнадзора) рекомендуется проведение следующего комплекса мероприятий:

1. Создание комиссии по проведению комплекса мероприятий по защите ПДн. Учитывая, что проведение данных работ включает широкий круг вопросов, в состав комиссии привлекаются лица, обладающие знаниями в сфере защиты информации, в области юриспруденции, работника кадровой службы, бухгалтера, системного администратора.
2. Начинать работу по проведению комплекса мер по защите ПДн следует с проведения категорирования обрабатываемых персональных данных. Проще говоря, задачей данного этапа работы является выявление всех данных персонального характера, обрабатываемых в организации. Также на данном этапе необходимо оценить наличие согласий субъектов ПДн на обработку данных, проанализировать требуется ли для нужд организации хранение всех

сведений персонального характера, а также определить перечень ответственных лиц.

3. Определение характеристики ИСПДн. На данном этапе необходимо определить конфигурации и топологии ИСПДн, физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения, определить технические и программные средства, используемые в ИСПДн.

4. Определение перечня угроз в части соблюдения безопасности информации, их актуальность (рекомендуется привлечение экспертов по информационной безопасности), разработка модели угроз и определение класса ИСПДн.

5. Подготовка и направление уведомления в Роскомнадзор с целью включения в реестр операторов.

6. Разработка порядка работы с ПДн. В случае необходимости разработать и провести комплекс дополнительных мероприятий по защите ПДн, в том числе по технической защите ПДн (приобрести и настроить необходимые технические средства и программное обеспечение).

Разработанный порядок должен обеспечивать своевременное предоставление информации в случае получения запросов из Роскомнадзора (7 раб. дней) или непосредственно от физических лиц - субъектов ПДн (10 раб. дней).

7. Подготовка и утверждение комплекта организационно-распорядительной документации. В наличии должны быть:

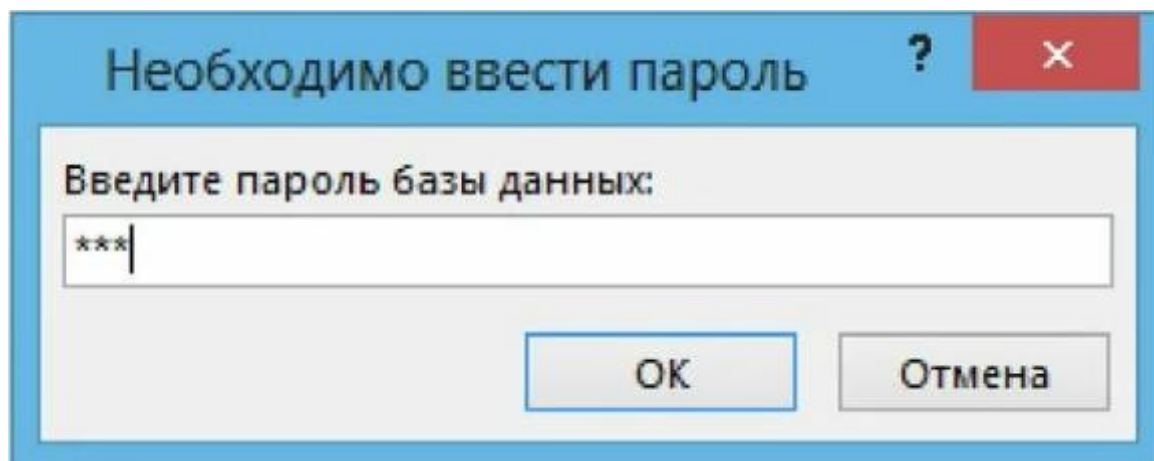
- Приказ о назначении ответственного должностного лица/подразделения; - Положение о защите ПДн;
- Приказы о допуске, перечень допущенных сотрудников;
- Журналы учета носителей информации.

8. Доведение до сотрудников порядка работы со сведениями о персональных данных, в том числе обучение сотрудников.

9. Планирование и проведение контрольных мероприятий по защите ПДн.

### **Практическая работа № 3. «Парольная защита».**

Самая распространенная защита компьютерной информации - защита на основе пароля. При реализации парольной защиты вход в систему, запуск приложения, запрос на доступ к данным сопровождается запросом пароля и последующим сравнением введенного пароля с оригиналом.



*Пароль представляет собой последовательность символов некоторого алфавита и специальных знаков. Последовательность должна удовлетворять ограничению на наименьшую и наибольшую длину.*

Сразу заметим, что парольная защита может быть рекомендована только для использования при защите информации, предназначенной для узкого круга пользователей. При широком использовании, например, программ, защищенных таким образом, очень велика вероятность того, что хотя бы один законный пользователь сообщит пароль злоумышленнику, этого будет достаточно для того, чтобы сделать защищенное приложение общедоступным.

Следует обратить внимание на то, что процесс ввода пароля поддается наблюдению. Человек, находящийся рядом с пользователем, вводящим пароль, наблюдая за процессом набора на клавиатуре, может зафиксировать вводимые символы. Кроме того, существует множество специальных программ типа «троянский конь», которые через перехват соответствующего прерывания читают и сохраняют пароли, набираемые на клавиатуре.

Хорошая система защиты организована таким образом, что, во-первых, не позволяет пользователю бесконечно вводить неправильный пароль, а ограничивает число попыток. Во-вторых, между двумя неудачными попытками ввода пароля специально вводится временная задержка с целью уменьшить количество попыток взлома системы защиты за некоторый промежуток времени.

Даже начинающим программистам известно, что нельзя хранить пароль в открытом виде.

Так как, например, в случае хранения пароля непосредственно в защищаемой программе злоумышленник может легко найти эталонный пароль.

Идентификация используется для определения, существует ли конкретный пользователь в системе. Проводится, например, по номеру телефона или логину. Аутентификация — это процесс подтверждения права на доступ с помощью ввода пароля, пин-кода, использования биометрических данных и других способов.

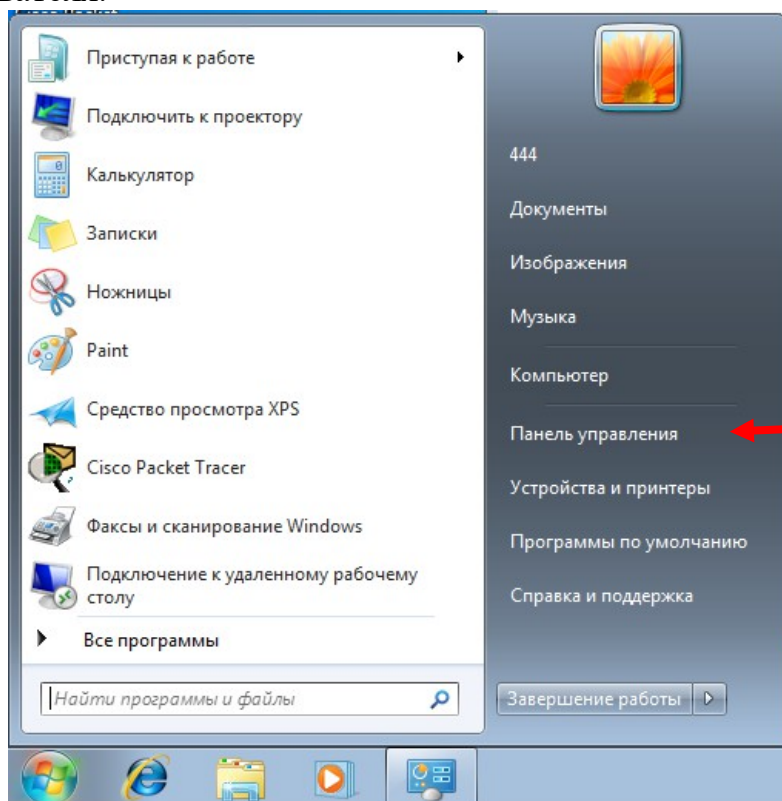
- пароль должен быть обязательно сложным, а именно содержать буквы, цифры и специальные символы;
- использовать всегда уникальные пароли на разные аккаунты, сайты и приложения;
- не хранить пароли на бумажных носителях, предметах размещающихся на рабочем месте и на мобильных носителях информации не защищенных от внешнего несанкционированного доступа;
- при сохранении паролей на облачном хранилище не забывайте использовать максимально сложный пароль для доступа к нему;

Для создания сложного пароля можно использовать разные сервисы по генерации паролей, для примера вот два сайта для генерации пароля:

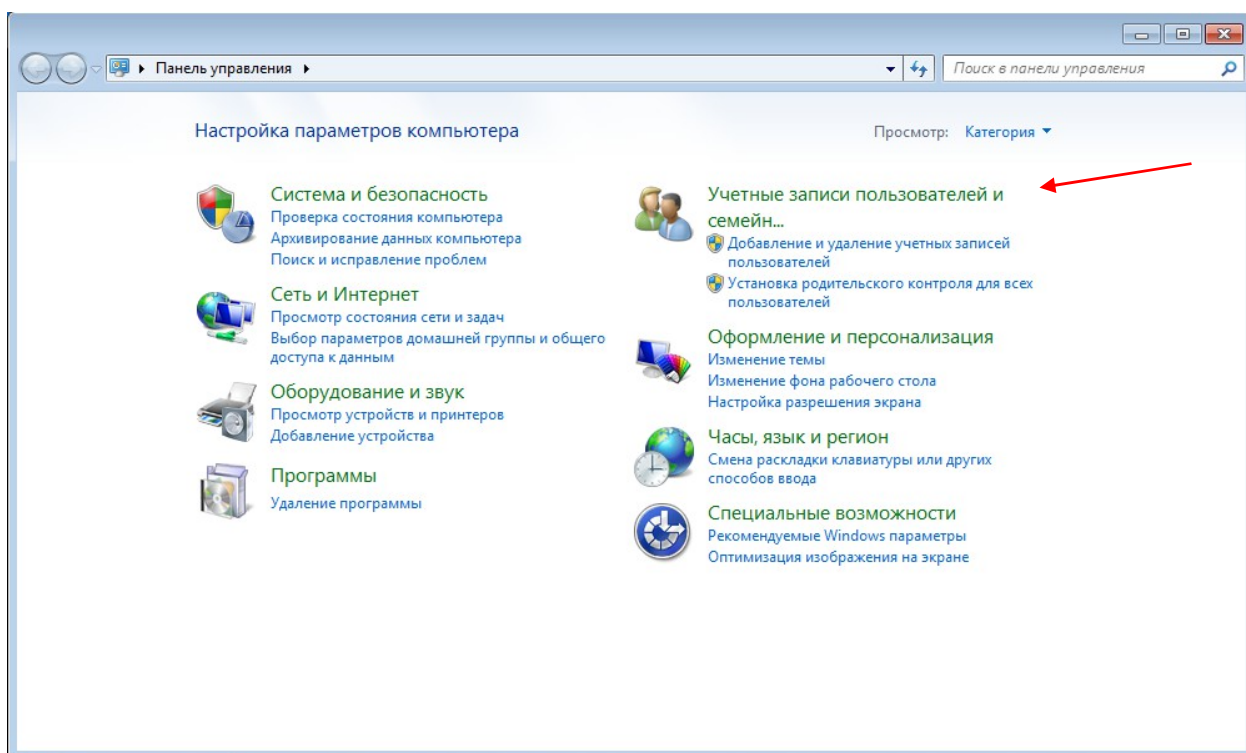
- 1) <https://randstuff.ru/password/>
- 2) <http://passgen.ru/>

### **ПРИМЕР: Создание учетной записи в операционной системе Windows 7 с помощью виртуальной машины Oracle Virtual Box**

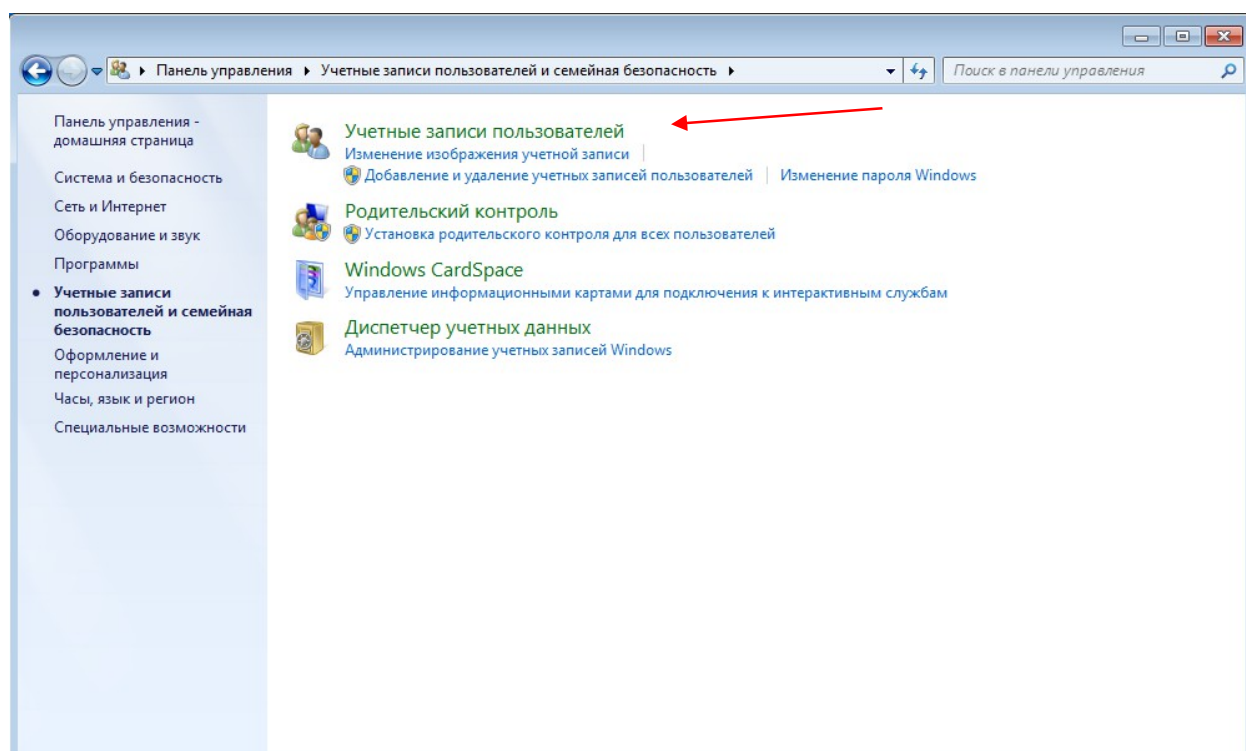
В данном примере будет показано, как можно создать Учетную запись другому пользователю, ограничить, или дать больше возможностей пользователю вносить изменений в ОС, а так же как удалить Учетную запись пользователя.



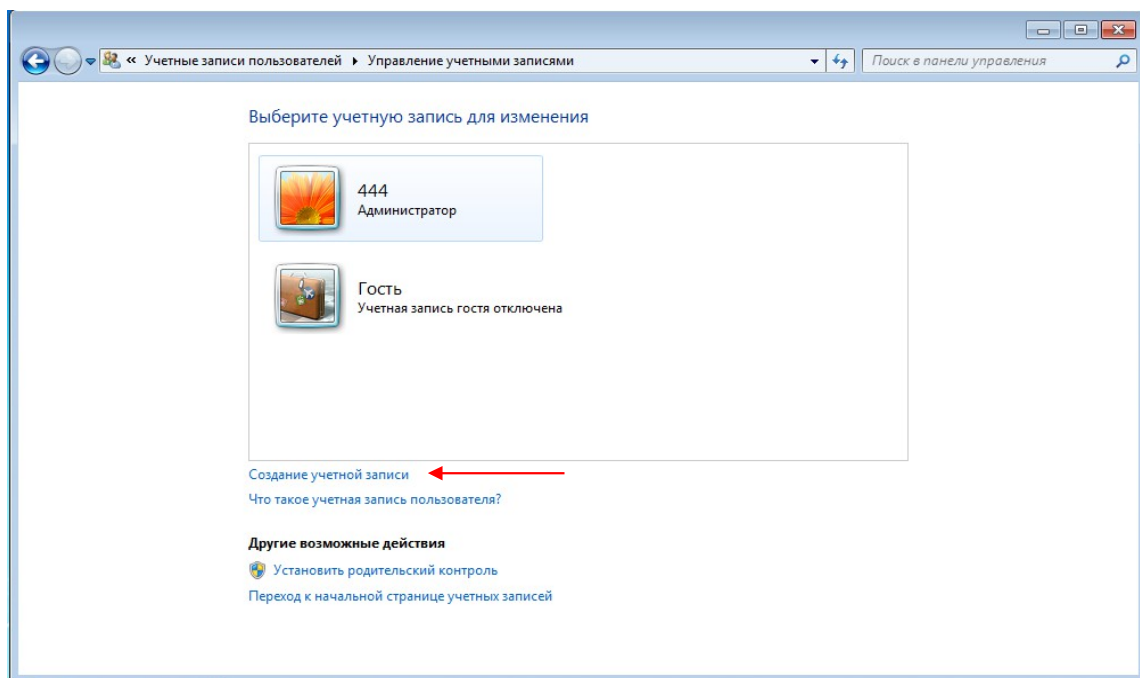
1) Нажимаем на иконку «Пуск» в левом нижнем углу, после нажимаем на «Панель управления»



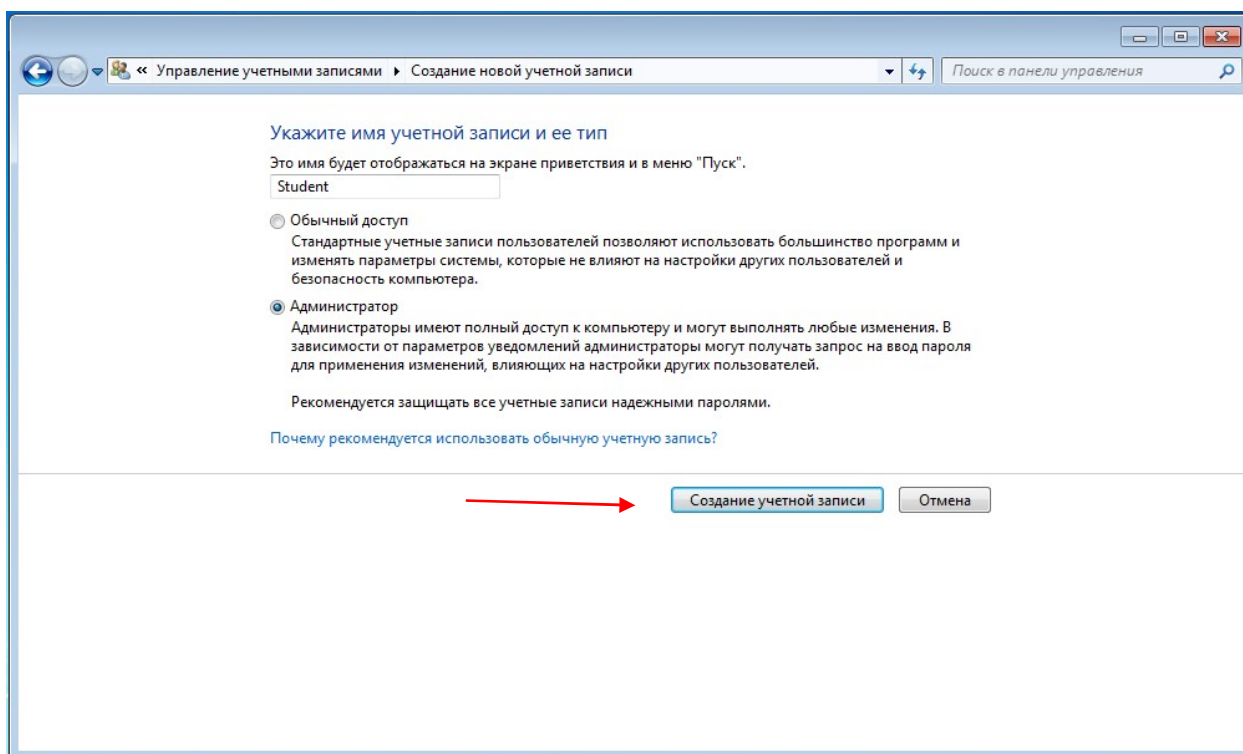
2) В открывшемся окне нажимаем на «Управление записями пользователей и семейная безопасность»



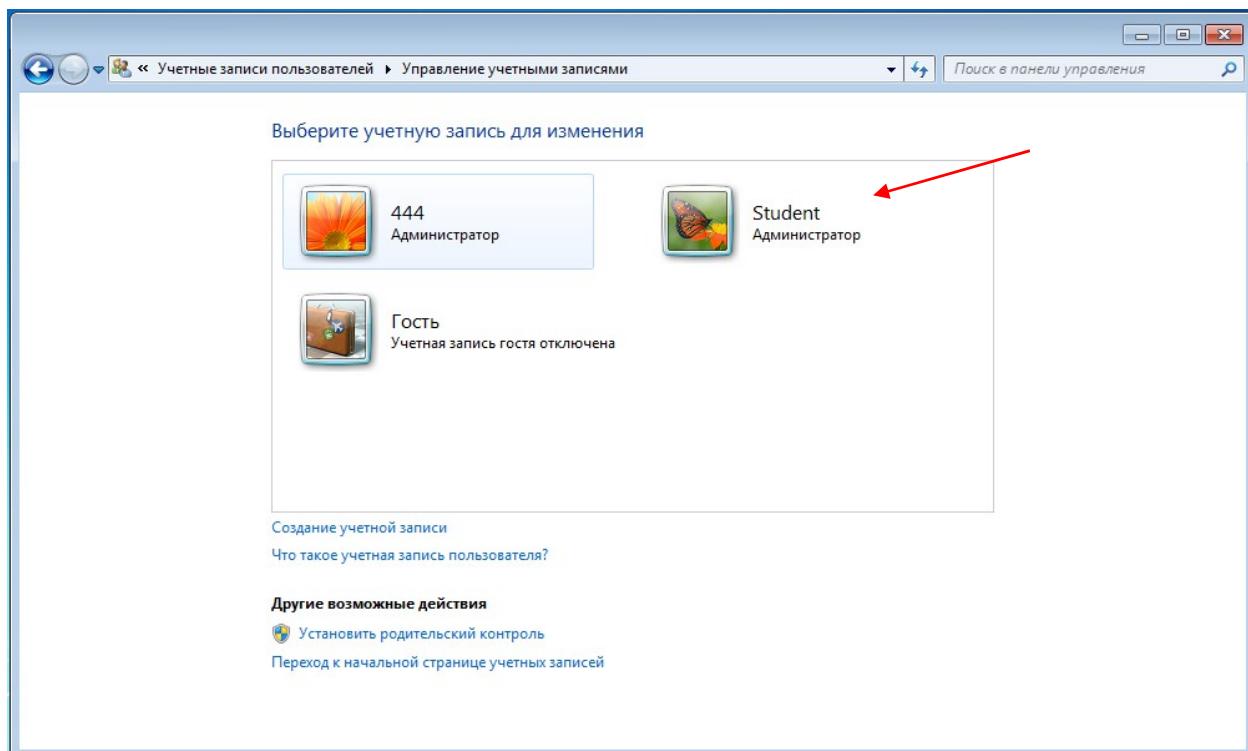
- 3) Далее нажимаем на «Учетные записи пользователей»
- 4) Нажимаем на «Управление другой учетной записью»



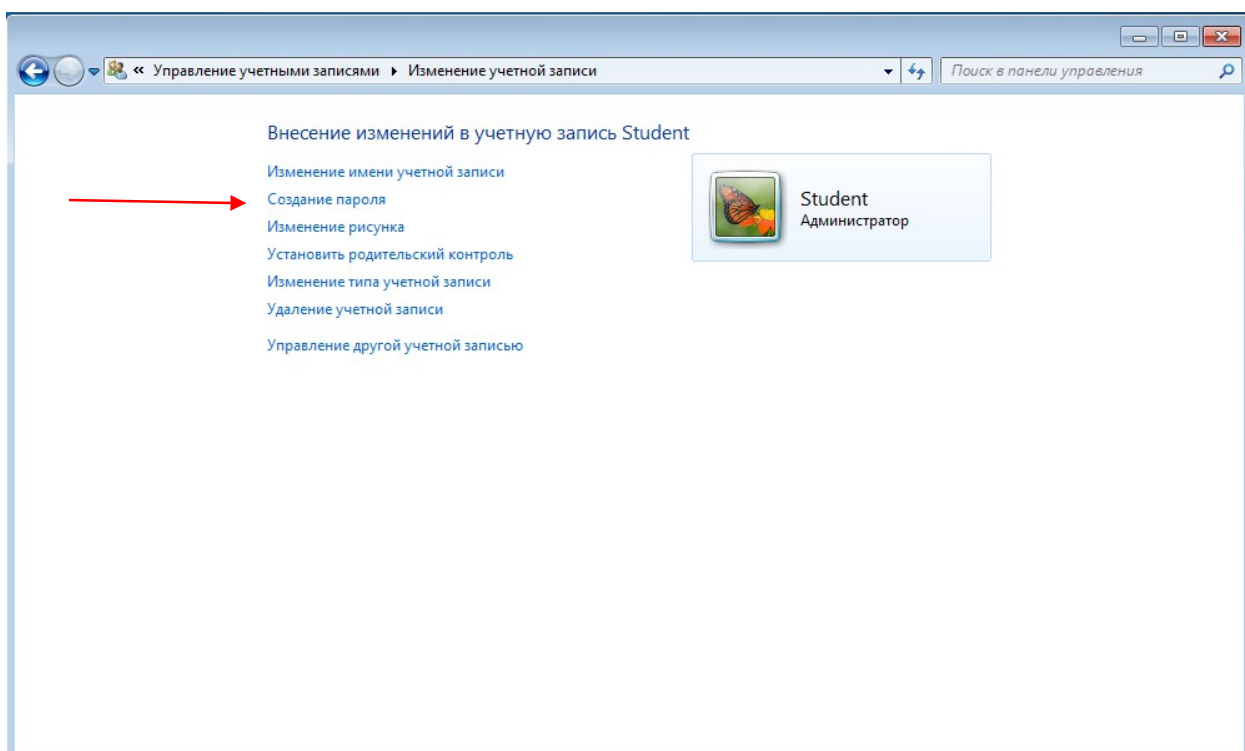
- 5) Нажимаем на «Создание учетной записи»



- 6) Пишем имя Учетной записи, выбираем какие права доступа дать. В примере выбираются права «Администратора». После нажимаем кнопку «Создание учетной записи»

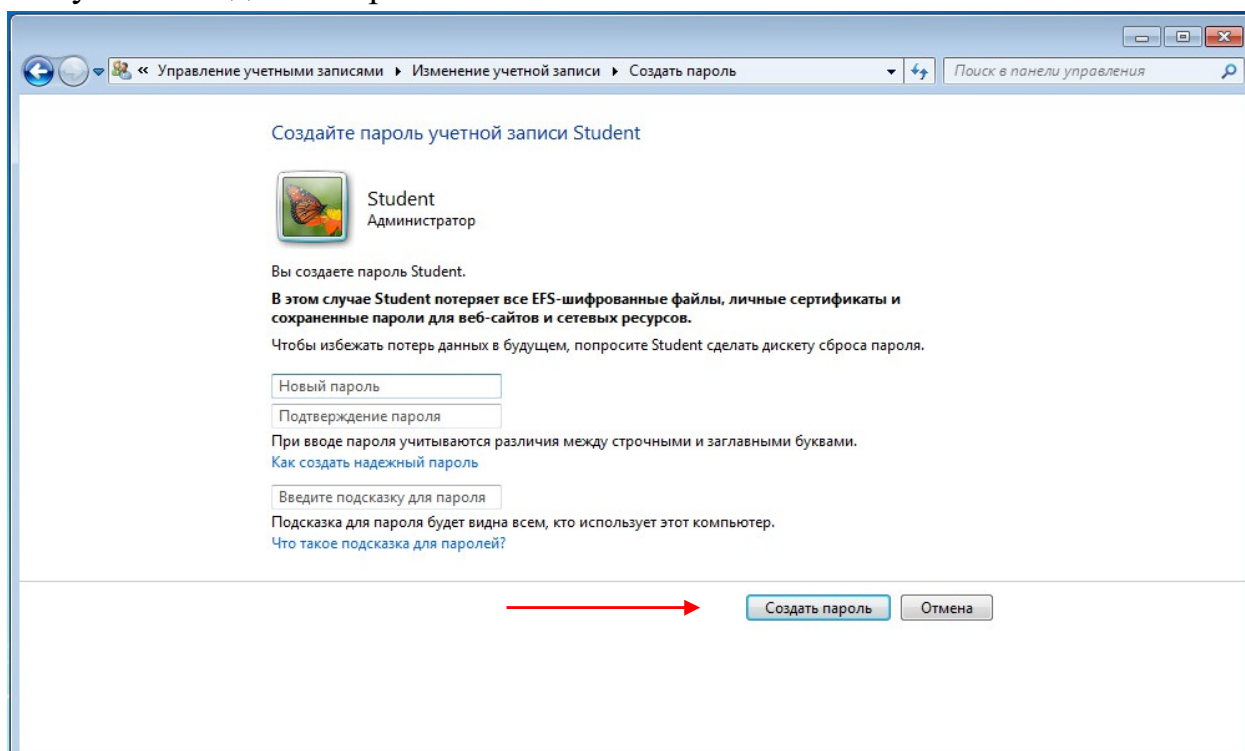


7) После мы можем наблюдать, как появилась новая учетная запись пользователя «Student». Нажимаем на новую Учетную запись «Student»

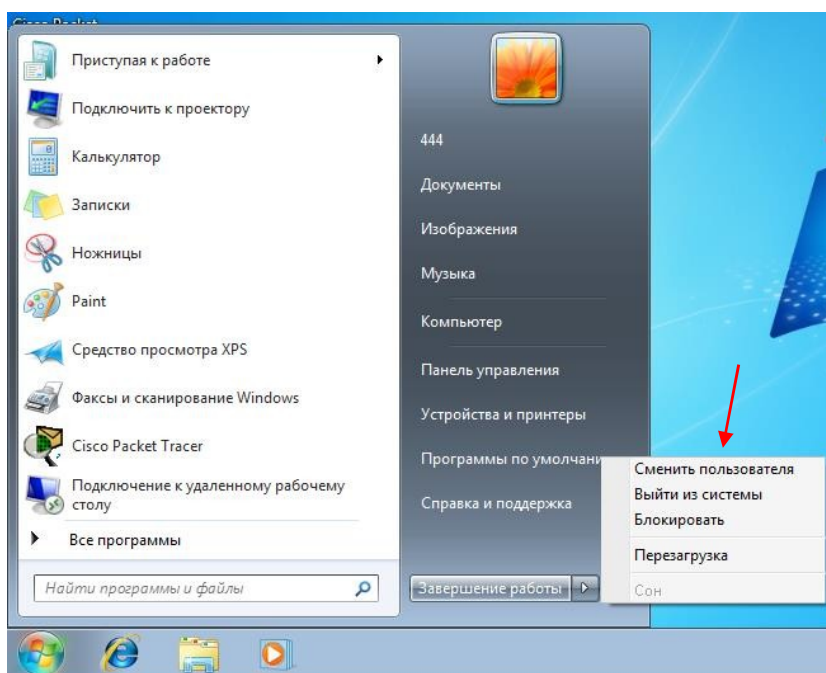


8) Тут можно производить различные настройки Учетной записи, но только если вы обладаете правами Администратора (Зашли в Windows под пользователем с правами Администратора). Нажимаем на

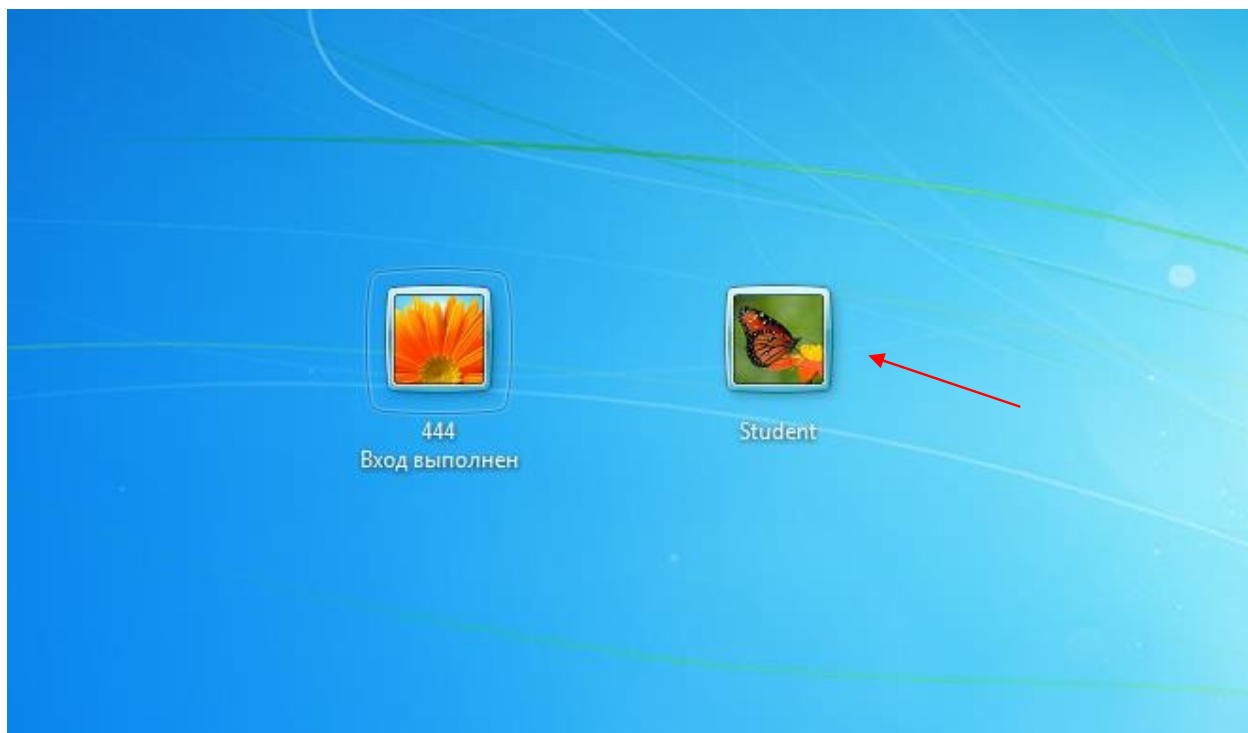
## пункт «Создание пароля»



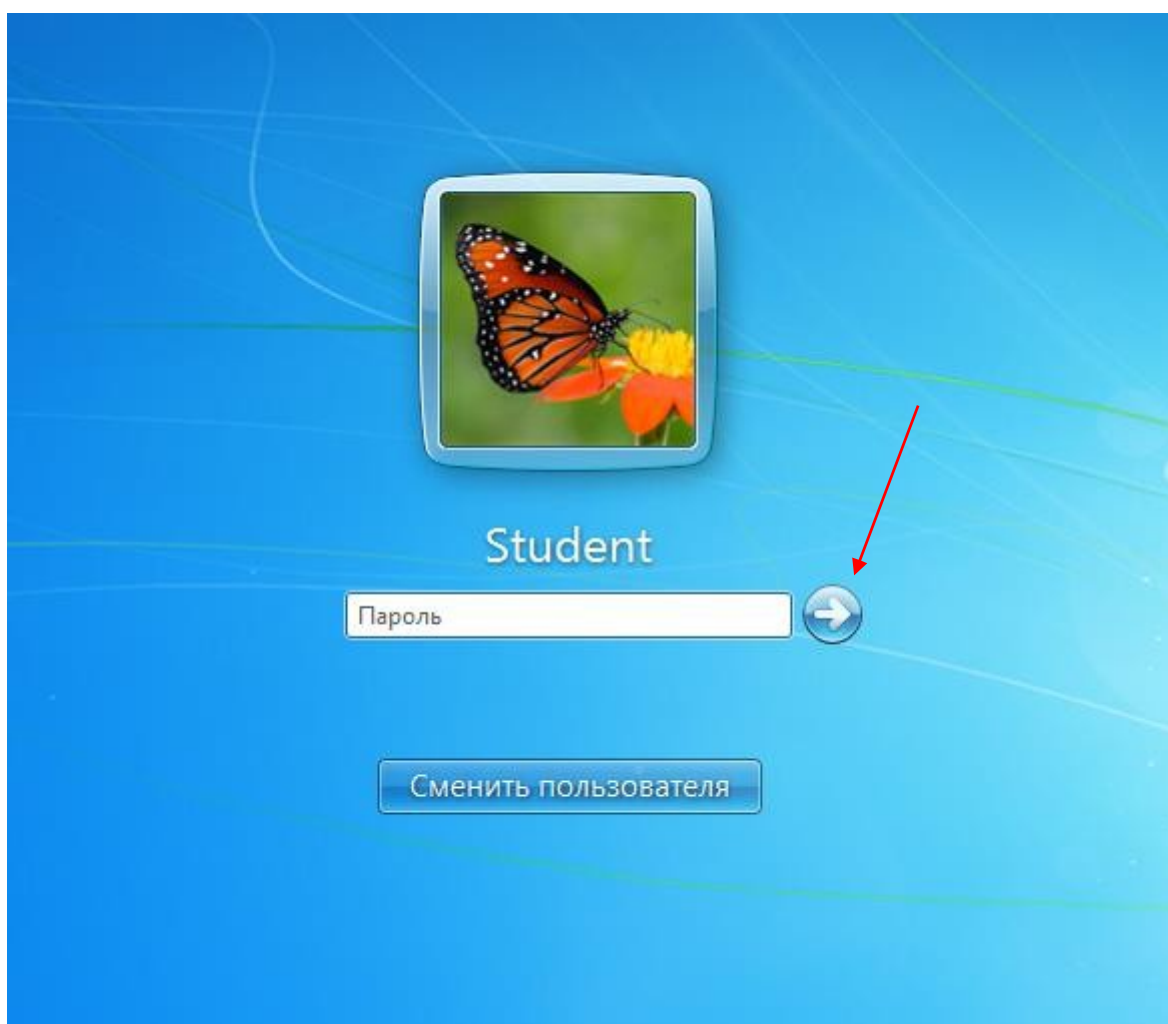
9) Вводим пароль, который придумали или который сгенерировали с помощью программ



10) Нажимаем на «Пуск», рядом с кнопкой завершить сеанс есть треугольник, при нажатии на него откроется список, в нём нажимаем на «Сменить пользователя»

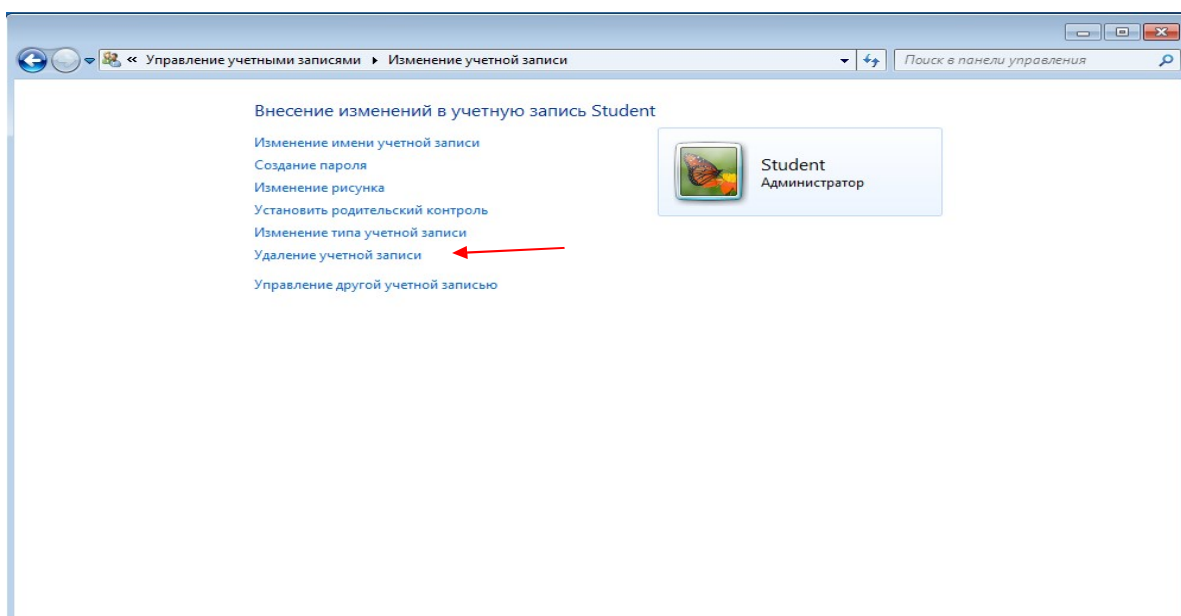


11) Выбираем пользователя, которого создали.

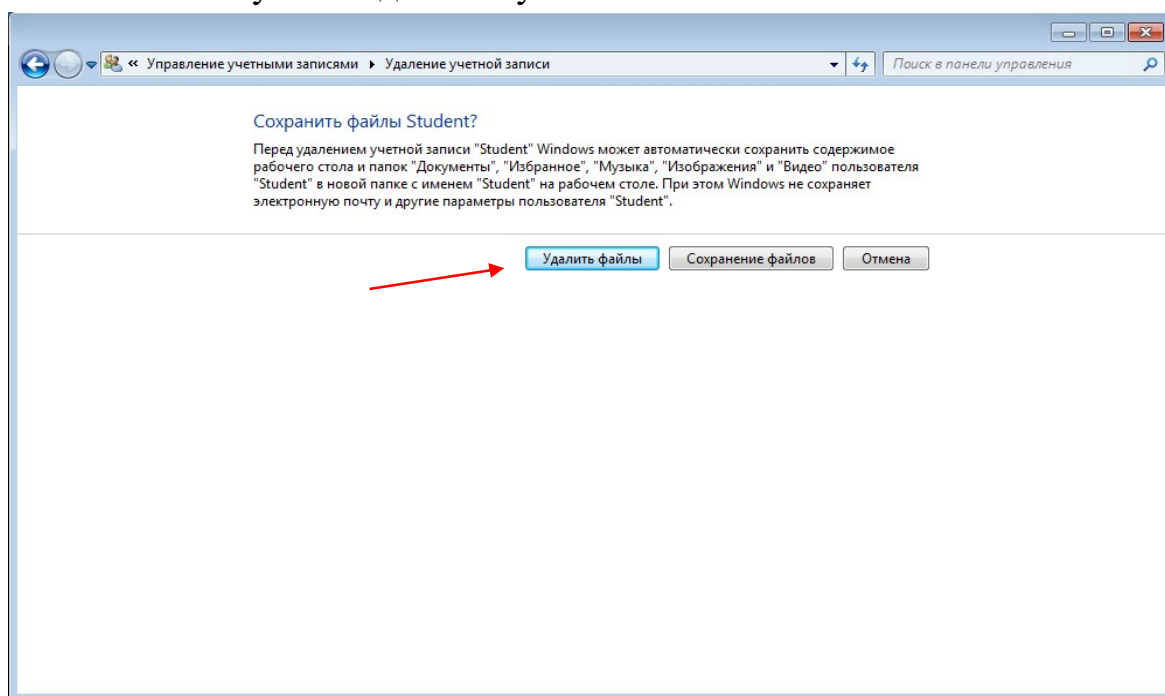


Вводим пароль. Таким образом, мы создали Учетную запись для другого пользователя который сможет заходить в ОС под собой.

Далее будет показан способ удаления Учетной записи.

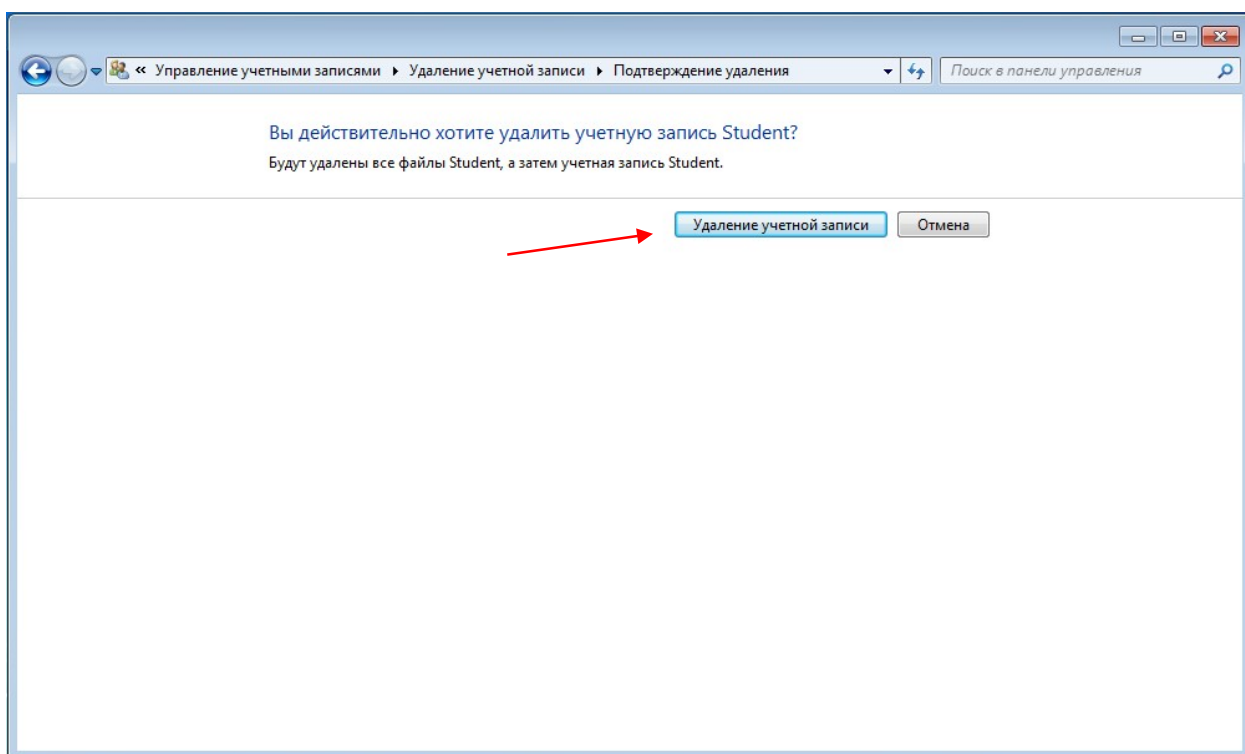


12) Заходим в ОС под пользователем с правами Администратора (не под тем пользователем, которого хотим удалить) Попасть в этот раздел можно сделав действия по «Примеру выше с 1 по 4 и 7 картинку. Нажимаем пункт «Удаление учетной записи»



13) Тут нам предлагают сохранить или удалить файлы, которые были созданы пользователем в определенных местах. Мы

выбираем «Удалить файлы»



Повторное предупреждение. Нажимаем «Удаление учетной записи».

#### **Практическое занятие № 4 Политика «Требования по обеспечению информационной безопасности»**

Цель занятия: рассмотрение основных и наиболее важных моментов при разработке политики «Требования по обеспечению информационной безопасности» для выбранной КИС.

Задачи: формализовать требования по обеспечению безопасности ресурсов КИС в соответствии с действующим законодательством [1, 9].

#### Ход работы

«Требования по обеспечению информационной безопасности (ИБ)» для выбранной КИС. Выделим следующие разделы для будущего документа:

1. Общие положения;
2. Рабочее место пользователя;
3. Парольная политика;
4. Работа с электронной почтой;
5. Работа в сети Интернет;
6. Действия в нестандартных ситуациях;
7. Ответственность.

Ниже подробно рассмотрим содержание перечисленных разделов с представленными в скобках примерами. Отметим сразу, что результаты по ходу работы будем заносить в форму 1

## Форма для заполнения к практическому занятию № 1

ФИО студента, группа \_\_\_\_\_

Политика «Требования по обеспечению информационной безопасности»

В \_\_\_\_\_

### 1. Общие положения

1.1. \_\_\_\_\_

1.2. \_\_\_\_\_

1. .. \_\_\_\_\_

### 2. Рабочее место пользователя

2.1. \_\_\_\_\_

2.2. \_\_\_\_\_

2... \_\_\_\_\_

### 3. Парольная политика

3.1. \_\_\_\_\_

3.2. \_\_\_\_\_

3... \_\_\_\_\_

### 4. Работа с электронной почтой

4.1. \_\_\_\_\_

4.2. \_\_\_\_\_

4... \_\_\_\_\_

### 5. Работа в сети Интернет

5.1. \_\_\_\_\_

5.2. \_\_\_\_\_

5. .. \_\_\_\_\_

### 6. Действия в нестандартных ситуациях

6.1. \_\_\_\_\_

6.2. \_\_\_\_\_

6... \_\_\_\_\_

### 7. Ответственность

7.1. \_\_\_\_\_

7.2. \_\_\_\_\_

7. .. \_\_\_\_\_

#### **Рабочее место пользователя**

Начнем разработку нашей политики с данного раздела, в котором отметим следующие моменты:

Правила предоставления сотруднику рабочего места и ограничение прав на его эксплуатацию (Для выполнения своих должностных обязанностей сотруднику компании выделяется персональный компьютер (ПК) с предустановленным программным обеспечением (ПО) и доступом к локально-вычислительной сети (ЛВС) компании. ПК предоставляется сотруднику во временное пользование на период работы в организации и должен использоваться им для служебных целей. Установку, настройку, а также подключение к ЛВС выполняют только сотрудники, уполномоченные на перечисленные операции);

Исходя из важности обеспечения сохранности информации, введем правило создания резервной копии (*Сотрудник должен периодически (как часто?) создавать резервные копии, сохраняя важную информацию в выделенной папке файлового сервера компании; резервная копия информации создается автоматически (как часто и какие действия необходимы со стороны сотрудника для исключения ошибок)*);

Исключения доступа к рабочему месту сотрудника посторонних лиц (*Оставляя рабочее место, даже на короткое время, пользователь обязан заблокировать доступ к работающему ПК (можно использовать средства операционной системы или, в случае наличия, средствами защиты информации, которыми оснащен ПК)*);

Действия, которые запрещено производить сотрудникам (*Открывать корпус ПК и изменять его конфигурацию; Несанкционированно изменять настройки ПО, параметры доступа к ресурсам КИС; Отключать антивирусное ПО, а также предусмотренные средства защиты; Подключать к ЛВС несанкционированное оборудование (Например, активное сетевое оборудование, незарегистрированные компьютеры и т.д.); умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты; Осуществлять действия, направленные преодоление систем безопасности, получение несанкционированного доступа к ресурсам КИС, ухудшение рабочих характеристик КИС, перехват информации, циркулирующей в КИС; Оставлять переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже (можно ввести правило использования замков для переносных компьютеров или требование по помещению их в закрывающийся на ключ шкаф на время обеденного перерыва и после окончания рабочего дня); Осуществлять обработку информации ограниченного доступа на ПК в присутствии лиц, не уполномоченных для доступа к данной информации, если при этом указанные лица смогут ознакомиться с обрабатываемой информацией; Несанкционированно записывать и хранить информацию на неучтенных носителях информации, а также оставлять без личного присмотра на рабочем месте носители информации и распечатки, содержащие информацию ограниченного доступа; Хранить и обрабатывать развлекательные мультимедийные файлы в КИС; Допускать к работе на ПК лиц, не имеющих прав доступа в КИС).*

### **Парольная политика**

Для предотвращения несанкционированного доступа к ресурсам КИС используются пароли и/или аппаратные средства аутентификации.

Рассмотрим основные правила, которые должен выполнять сотрудник организации:

Сотрудники обязаны обеспечить безопасное хранение *пароля и/или средства аутентификации*, исключаяющие их утерю или разглашение;

Рекомендуется изменять пароли с периодичностью *не более 90 дней*, при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3-х позициях;

Запрещается сообщать кому-либо, даже администраторам сети, свой пароль для доступа к информационным ресурсам КИС;

В случае подозрения на разглашение пароля необходимо немедленно изменить пароль и проинформировать начальника (*своего отдела, отдела безопасности*);

Требования, в соответствии с которыми сотрудник обязан создавать пароль (пароль должен состоять не менее чем из *восьми* символов; пароль не должен быть легко угадываемым (*пароль не должен включать повторяющуюся, последовательность каких-либо символов (например, «111111», «aaaaaa», «12345», «qwerty», «йцукен» и т.п.*), пароль не должен включать в себя легко подбираемые сочетания символов (*имена, фамилии, наименования, клички домашних животных, даты рождения и т.д.*) и общепринятые сокращения (*ЭВМ, ЛВС, USER и т.п.*));

### **Работа с электронной почтой**

При эксплуатации электронной почты, сотрудники обязаны выполнять следующие требования:

Допускается использовать корпоративную электронную почту только для выполнения своих служебных обязанностей;

Запрещается самовольно менять настройки почтовой системы;

Запрещается отправлять сообщения противозаконного, враждебного или неэтического содержания;

Запрещается использовать публичные сервисы электронной почты (*например, Yahoo, Mail, Yandex и др.*) для осуществления корпоративной деятельности;

Для защиты сообщений от подмены, модификации и прочтения третьими лицами следует использовать *средства шифрования электронной почты и электронной подписи*;

При получении электронных содержаний сомнительного содержания и/или из незнакомого источника не следует открывать файлы, вложенные в сообщение, так как они с большой вероятностью могут содержать вирусы. *Такие сообщения необходимо удалять*;

Не следует отвечать на подозрительные письма, а также сообщать любые данные о себе, если сотрудник не доверяет отправителю письма;

Запрещается в личных целях публиковать личный корпоративный адрес сотрудника при заполнении анкет, так как эти данные могут быть использованы для рекламных рассылок;

Запрещается самостоятельно настраивать и включать автоматическую пересылку сообщений корпоративной электронной почты на внешние адреса электронной почты.

### **Работа в сети Интернет**

При использовании Интернет, пользователи обязаны выполнять следующие требования:

допускается использовать ресурсы Интернет только для выполнения своих служебных обязанностей;

запрещается посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтического характера, использовать доступ в Интернет в развлекательных целях;

запрещается несанкционированно размещать какую-либо информацию в Интернет;

запрещается использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом;

запрещается несанкционированно загружать программы из сети Интернет и запускать их;

запрещается осуществлять попытки несанкционированного доступа к защищенным ресурсам Интернет (*перебор паролей, использование уязвимостей и неправильных настроек информационных систем*);

запрещается осуществлять туннелирование сетевого трафика при обращении к ресурсам сети Интернет через корпоративные прокси сервера;

запрещается несанкционированное использование систем мгновенного обмена сообщениями (*Instant Messaging*),

систем передачи голоса по IP-протоколу (*VOIP*), систем видеосвязи по IP-протоколу (*Skype*), систем для удалённого доступа и общего доступа к рабочему столу.

### **Действия в нестандартных ситуациях**

Сотрудники, пользующиеся ресурсами КИС обязаны немедленно ставить в известность своего непосредственного руководителя и/или начальника отдела информационной безопасности и технической защиты, в случае возникновения или возможного возникновения следующих событий:

разглашения учетных данных; потери, кражи средств аутентификации;

несанкционированных (*произведенных с нарушением установленного порядка*) изменений в конфигурации программных или аппаратных средств рабочей станции;

фактов совершения попыток несанкционированного доступа к ресурсам КИС;

фактов потери, кражи компьютеров или носителей информации, особенно если они содержали информация ограниченного доступа;

заражение ПК пользователя вирусами;

сбоев в работе средств защиты информации;

в любых других случаях, если, по мнению пользователя, возникают риски нарушения безопасности информации.

### **Ответственность**

Ответственность за выполнение требований Политики возлагается на всех работников, являющихся пользователями КИС.

Любой работник компании, нарушивший требования данной политики, может быть, подвергнут дисциплинарному наказанию, в соответствии с законодательством РФ и трудовым договором.

### **Общие положения**

Итак, разработав основные разделы политики, вернемся к общим положениям. В данном разделе должны быть отражены следующие моменты:

На кого будет распространяться данный документ (*все пользователи КИС; персонал, непосредственно работающий с клиентами*) и в какой момент они должны с ним ознакомиться (*только при получении первичного доступа к КИС, при получении первичного доступа к КИС, а также ежегодно в рамках проведения внутренних профилактических работ по обеспечению ИБ*);

Необходимо предупредить работников организации об ответственности и обязанности соблюдения установленных документом правил (*каждый пользователь несет персональную ответственность за свои действия и обязан строго соблюдать установленные правила по работе с программными и техническими средствами*);

Обоснование уникальных учетных записей (*С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю назначается персональное уникальное имя. Запрещается использовать чужую учетную запись, а также передавать кому-либо свои учетные данные*);

Ресурсы КИС предоставляются пользователям для осуществления ими своих обязанностей, связанных с деятельностью компании. При этом соблюдают принципы разумной достаточности и минимальной необходимости. (*Сотруднику компании разрешается пользоваться только той информацией и в том объеме, которые ему необходимы для выполнения своих должностных обязанностей. Сотрудник не имеет права предпринимать попыток получить доступ к ресурсам КИС, не пройдя процедуру официального получения разрешения на доступ к ресурсам.*);

Осуществление контроля за правильностью обработки информации, ввиду принадлежности информационных ресурсов организации (*Информация, циркулирующая в КИС, является собственностью компании. Компания оставляет за собой право протоколировать и контролировать действия работников при обработке информации в КИС*);

Необходимо минимизировать возможность внешнего проникновения в КИС (*Пользователи не должны разглашать информацию о процедурах и технической реализации защиты информации в КИС*);

Обязанность работников сообщать о фактах нарушения установленных в документе правил (*Пользователи должны информировать своего непосредственного руководителя и/или уполномоченного сотрудника отдела информационной безопасности и технической защиты обо всех фактах нарушения данной политики*).

## **Практическая работа № 5 Организация защиты информации на персональном компьютере**

### Практическая часть

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением

требований обеспечения безопасности информации;

- для формирования и реализации единой политики в области обеспечения информационной безопасности.

### Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании, содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

#### **1. Общие положения**

1.1. Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

#### **2. Проблемная ситуация в сфере информационной безопасности**

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.

- Основные непреднамеренные искусственные угрозы.

- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

#### **3. Механизмы обеспечения информационной безопасности Предприятия**

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

#### **4. Мероприятия по реализации мер информационной безопасности Предприятия**

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.

- Подразделения, занятые в обеспечении информационной безопасности.

- Взаимодействие подразделений, занятых в обеспечении

информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Пред-приятия.
- Правовое обеспечение юридических отношений с партнерами Пред-приятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

**5. Программа создания системы информационной безопасности Пред-приятия**

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании.

**Практическая работа №6 Выявление угроз информационной безопасности в конкретных ситуациях**

- изучить угрозы информационной безопасности
- научиться определять угрозы и способы их предотвращения

**Теоретические сведения**

*Информационный объект* – это среда, в которой информация создается, обрабатывается, хранится и передается.

Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу.

Рассмотрим их классификацию по различным классификационным признакам.

*По виду:*

- физической и логической целостности (уничтожение или искажение информации);
- конфиденциальности (несанкционированное получение);
- доступности;
- права собственности.

*По характеру:*

- случайные (отказы, сбои, ошибки, стихийные явления);
- преднамеренные (злоумышленные действия людей);

*источникам:*

- человек;
- технические устройства;
- программное обеспечение;
- внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

*Угроза конфиденциальности* – нарушение свойства информации быть известной только определенным субъектам.

*Угроза целостности* – несанкционированное изменение, искажение, уничтожение информации.

*Угроза доступности (отказ в обслуживании)* – нарушение работоспособности объекта, доступ к которому получил злоумышленник.

*Случайные угрозы* обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии.

*Преднамеренные угрозы* связаны с действиями людей (работники спецслужб либо самого объекта, хакеры).

Для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить:

- побочное электромагнитное излучение информации с аппаратуры системы;
- побочные наводки информации по сети электропитания и заземления;
- побочные наводки информации на вспомогательных коммуникациях;

- подключение к внешним каналам связи.

В таблице 2 представлена подробная классификация угроз информационной безопасности в зависимости от их источника и происхождения

Таблица 2

Классификация угроз информационной безопасности

| Природные угрозы                                                                                                                       | Угрозы техногенного характера                                                                                                                                                                                                          | Угрозы, созданные людьми                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• магнитные бури; – радиоактивные излучения и осадки;</li> <li>• стихийные бедствия.</li> </ul> | <ul style="list-style-type: none"> <li>– сбои в работе компьютерной сети (КС), вызванные отключением или колебанием электропитания либо другими средствами функционирования КС;</li> </ul>                                             | <ul style="list-style-type: none"> <li>– непреднамеренные либо преднамеренные действия:</li> <li>а) обслуживающего персонала;</li> <li>б) пользователей;</li> </ul>       |
|                                                                                                                                        | <ul style="list-style-type: none"> <li>• отказы и сбои КС вследствие её ненадёжности;</li> <li>• электромагнитные излучения и наводки;</li> <li>• утечки через каналы связи – электрические, акустические, оптические и др.</li> </ul> | <ul style="list-style-type: none"> <li>в) архивной службы;</li> <li>г) службы безопасности;</li> <li>д) управленческого персонала;</li> <li>– хакерские атаки;</li> </ul> |

Все методы защиты информации по характеру проводимых действий можно разделить на:

- законодательные (правовые);
- организационные;
- технические;
- комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации.

К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

### **Практическая работа №7. Определение функциональных возможностей и принципов работы троянской программы на примере клавиатурного шпиона**

**Цель:** Рассмотреть принцип работы и возможности троянской программы на примере клавиатурного шпиона

#### **Методические указания**

1. Установите в гостевой операционной системе клавиатурный шпион Elite Keylogger (ek\_setup.exe). При установке оставьте выбранным невидимый режим (invisible mode, по умолчанию). По окончании установки внимательно прочитайте Предупреждение (Warning), где написано, каким образом можно открыть программу (при необходимости сделайте снимок экрана с данным предупреждением). Подтвердите сообщение с предложением выполнить перезагрузку.

2. После перезагрузки войдите в систему под учётной записью пользователя, имеющего пароль.

3. Создайте на диске E: точечный рисунок произвольного содержания с использованием различных цветов и инструментов.

4. Войдите в систему под учётной записью Гуриева.

5. Запустите программу (ключевое слово нужно набрать с первой попытки, не прибегая к редактированию). После запуска установите и запомните пароль на её последующие запуски.

6. В разделе Logs нажмите кнопку View logs for <текущая дата> ... и сформируйте журнал событий за текущий день.

7. Найдите пароль пользователя, под именем которого вы входили в систему. Обратите внимание, зафиксирован он в программе полностью или частично.

8. Найдите снимки экрана (Screenshots), на которых зафиксирована работа пользователя.

### Ход работы

1. Установил ПО Elite Keylogger на виртуальной машине под управление ОС Windows 7. Рисунок 1

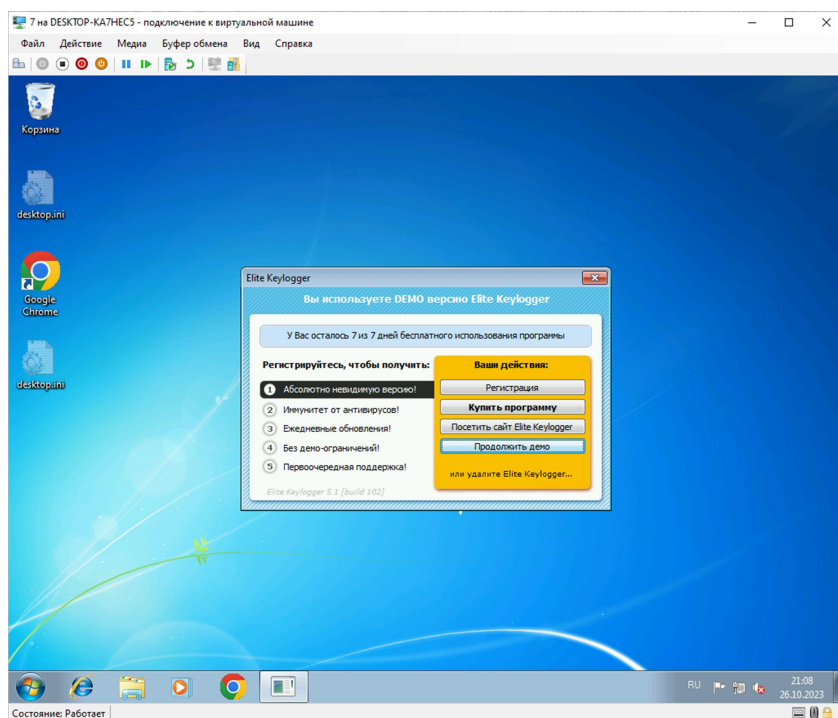


Рисунок 1

2. Имитировал работу настоящего пользователя. Программа сохраняет в логи введенные пароли, работу в файловой системе, произведенные пользователем. Рисунок 2.

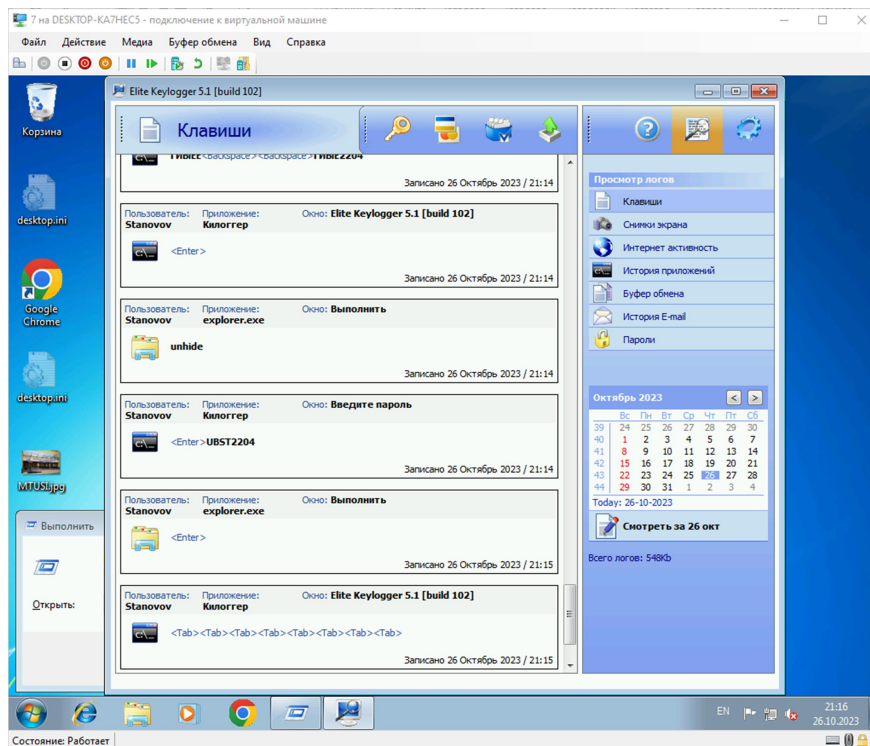


Рисунок 2

3. Имитировал работу настоящего пользователя. Программа сохраняет в логи снимки экрана, сделанные пользователем. Рисунок 3.

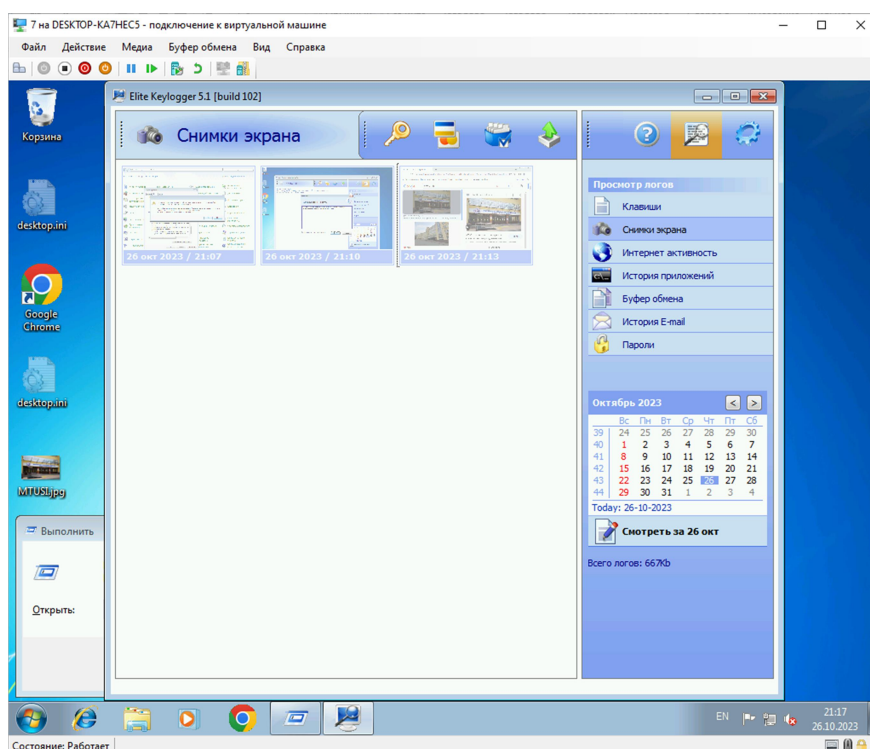


Рисунок 3

4. Создаю нового гостевого пользователя и имитирую деятельность обычного пользователя

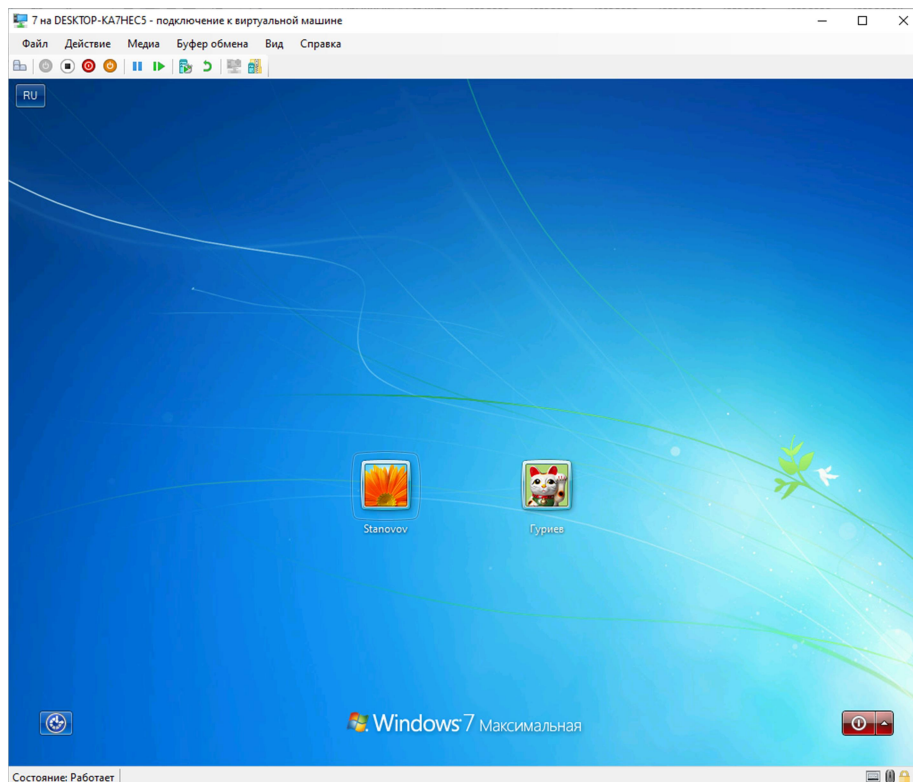


Рисунок 4

5. Проверяю работу программы. Установлено, что ПО аналогично считывает данные других пользователей. Рисунок 5.

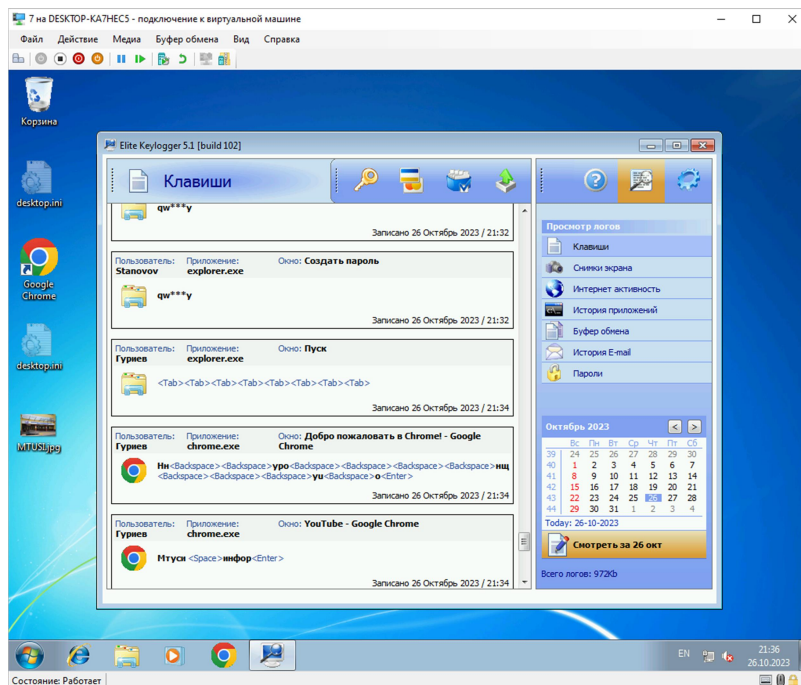


Рисунок 5

6. Проверяю историю приложений. Рисунок 6.

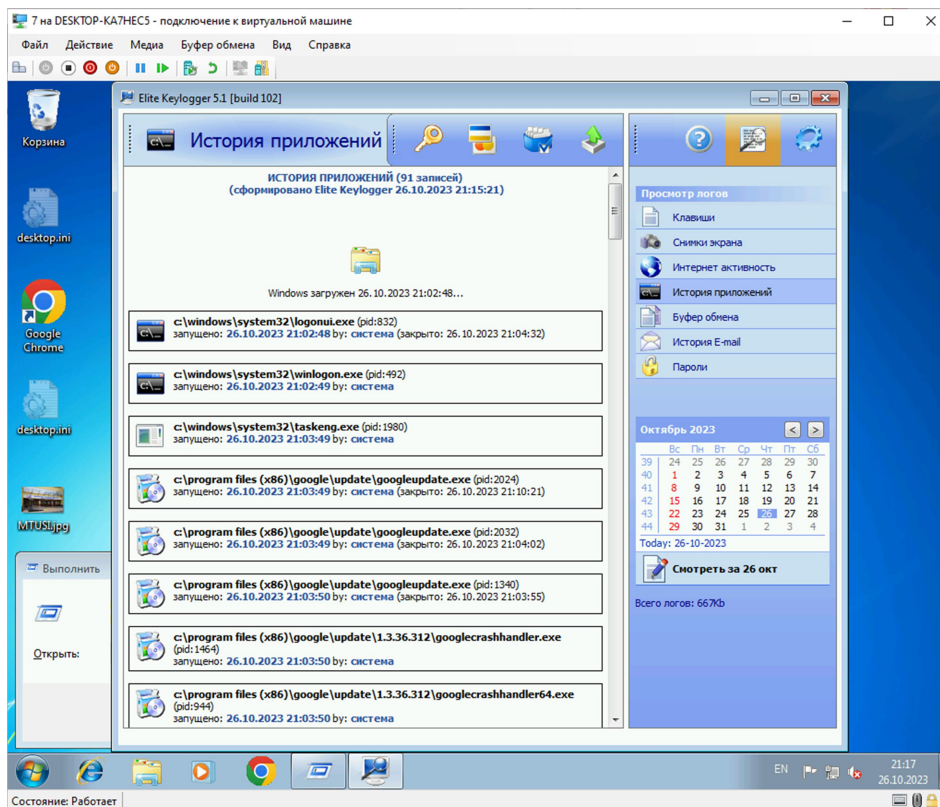


Рисунок 6

## Контрольные вопросы

### 1. Назовите типы клавиатурных шпионов.

- Клавиатурные шпионы, также известные как клавиатурные логгеры, представляют собой программное или аппаратное оборудование, предназначенное для записи нажатых клавиш на клавиатуре без согласия пользователя. Существует несколько типов клавиатурных шпионов:
  - Программные клавиатурные шпионы: Эти программы устанавливаются на целевом компьютере, обычно скрыто от пользователя, и записывают все нажатия клавиш. Затем они могут отправлять полученную информацию на удаленный сервер или хранить её на компьютере для последующего доступа.
  - Аппаратные клавиатурные шпионы: Это физические устройства, устанавливаемые между клавиатурой и компьютером. Они записывают все данные, проходящие через них, и могут быть позже извлечены злоумышленниками для анализа.
  - Wireless Keyloggers (Беспроводные клавиатурные шпионы): Эти устройства работают беспроводным способом и могут перехватывать данные, передаваемые между беспроводной клавиатурой и компьютером. Они обычно работают на частоте радиосигналов, которые используются для связи между клавиатурой и компьютером.

- Функциональные клавиатурные шпионы: Некоторые клавиатурные шпионы могут выполнять дополнительные функции, такие как перехват снимков экрана, запись звука или сбор данных о браузерной истории.

- Клавишные регистраторы в сети: Эти инструменты могут использоваться для мониторинга сетевых клавиатурных действий, таких как ввод паролей и логинов на веб-сайтах и в приложениях.

2. Перечислите разновидности программных и аппаратных клавиатурных шпионов.

Существует множество разновидностей программных и аппаратных клавиатурных шпионов, и их функциональность может варьироваться. Вот некоторые из распространенных разновидностей программных и аппаратных клавиатурных шпионов:

#### Программные клавиатурные шпионы

- Клавишные регистраторы общего назначения: Программы, которые скрыто записывают все нажатия клавиш на компьютере, включая пароли, текстовые сообщения и другие данные.

- Клавишные регистраторы сетевого трафика: Эти программы могут перехватывать данные, отправляемые и получаемые через сеть, включая вводимые пароли и текстовую информацию.

- Скриншотеры: Программы, которые регулярно делают снимки экрана, захватывая информацию, которая может включать в себя вводимый текст и изображения.

- Пульты дистанционного управления: Эти приложения позволяют злоумышленникам управлять компьютером издалека, включая наблюдение за клавишными действиями пользователя.

- USB-клавишные регистраторы: Программное оборудование, подключаемое к порту USB, которое записывает нажатия клавиш на клавиатуре.

#### Аппаратные клавиатурные шпионы

- Физические USB-клавишные регистраторы: Устройства, которые подключаются между клавиатурой и компьютером и записывают нажатия клавиш.

- Беспроводные клавишные регистраторы: Устройства, которые перехватывают беспроводные сигналы между беспроводными клавиатурами и компьютерами.

- Встроенные клавишные регистраторы: Аппаратные регистраторы, устанавливаемые непосредственно в клавиатуре и способные записывать нажатия клавиш, даже если они не подключены к компьютеру.

- Программируемые микросхемы в клавиатуре: Эти микросхемы могут быть встроены в клавиатуру и использоваться для записи клавишных действий.

- Клавишные регистраторы в виде дополнительных устройств: Например, устройства, которые могут быть установлены между монитором и компьютером и записывать данные, вводимые через клавиатуру.

### 3. Какие существуют способы распространения клавиатурных шпионов?

Существует несколько способов распространения клавиатурных шпионов, как программных, так и аппаратных. Вот некоторые из наиболее распространенных способов:

- Загрузка вредоносных веб-сайтов: Злоумышленники могут создавать вредоносные веб-сайты или внедрять вредоносные скрипты на легитимных сайтах. Посещение таких сайтов и взаимодействие с ними может привести к загрузке и установке программных клавиатурных шпионов на компьютер пользователя.

- Электронная почта: Злоумышленники могут отправлять вредоносные вложения или ссылки через электронную почту, которые, если пользователь их откроет, могут установить программные клавиатурные шпионы на компьютер.

- Социальная инженерия: Злоумышленники могут использовать манипулятивные методы, чтобы убедить пользователя скачать и установить вредоносное программное обеспечение, представляя его как полезное или необходимое.

- Уязвимости в программном обеспечении: Злоумышленники могут использовать известные или недавно обнаруженные уязвимости в операционных системах или приложениях, чтобы внедрить программные клавиатурные шпионы на компьютер без согласия пользователя.

- Сетевые атаки: Злоумышленники могут использовать методы, такие как атаки Man-in-the-Middle (человек посередине) или ARP-отравление, чтобы перехватывать сетевой трафик и собирать данные, включая вводимые с клавиатуры.

- Социальные сети и форумы: Злоумышленники могут использовать социальные сети и форумы для распространения вредоносных ссылок и вредоносных вложений, заманивая пользователей кликнуть на них.

- Физические аппаратные устройства: Аппаратные клавиатурные шпионы, такие как USB-клавишные регистраторы, могут быть физически подключены к компьютеру, когда злоумышленники имеют физический доступ к системе.

- Социальное инфильтрация: Злоумышленники могут попытаться стать частью организации или бизнеса и установить аппаратные клавиатурные шпионы, чтобы перехватывать данные.

- Вредоносные обновления программного обеспечения: Злоумышленники могут предложить фальшивые обновления для программного обеспечения, которые при установке устанавливают программные клавиатурные шпионы.

### 4. Какие наиболее популярные сферы использования клавиатурных шпионов вам известны?

Клавиатурные шпионы могут использоваться в разных сферах, как в легитимных, так и в незаконных целях. Вот некоторые из наиболее популярных сфер использования клавиатурных шпионов:

- Кибербезопасность и исследования: В области кибербезопасности клавиатурные шпионы могут использоваться исследователями и специалистами по безопасности для анализа угроз и выявления уязвимостей. Они могут также использоваться для мониторинга безопасности сетей и систем.
- Родительский контроль: Родители могут использовать клавиатурные шпионы для отслеживания активности своих детей в сети, чтобы обеспечить их безопасность и защитить их от нежелательных контактов и контента.
- Сотрудники и мониторинг производительности: Некоторые компании могут использовать клавиатурные шпионы для мониторинга активности сотрудников на рабочих компьютерах, чтобы следить за производительностью и обеспечивать безопасность корпоративной информации.

5. Перечислите методы защиты от клавиатурных шпионов.

Защита от клавиатурных шпионов играет важную роль в обеспечении безопасности ваших данных и личной информации. Вот некоторые методы защиты от клавиатурных шпионов:

1. Используйте надежное антивирусное программное обеспечение
2. Обновляйте программное обеспечение
3. Используйте брандмауэр
4. Осторожность при открытии вложений и ссылок
5. Используйте двухфакторную аутентификацию
6. Шифруйте свои данные
7. Мониторьте активность на компьютере
8. Не подключайте ненадежные устройства
9. Используйте безопасные сети Wi-Fi
10. Обучение и информирование
11. Активируйте средства безопасности в браузере
12. Регулярно сканируйте компьютер

### **Практическая работа №8. Выполнение установки антивирусного программного обеспечения**

**Цель:** Научиться устанавливать и настраивать антивирусное программное обеспечение.

Антивирусом называют специализированную программу, в функции которой входит обнаружение и удаление вредоносных приложений на компьютере. Кроме этого, антивирусы выполняют функцию восстановления зараженных файлов.

Большинство компаний, разрабатывающих антивирусное программное обеспечение, выпускают свою продукцию под операционные системы Windows.

Связано это с тем, что большая часть вирусных программ разрабатывается именно под эту платформу, просто потому что Windows, это наиболее популярная и наиболее распространенная система.

Изменить переключатель на «Защита файловой системы в режиме реально времени».

## Ход работы

1. Скачиваю и устанавливаю указанное ПО. Рисунок 1,2 - Процесс установки и настройки Антивирусного ПО ESET NOD32

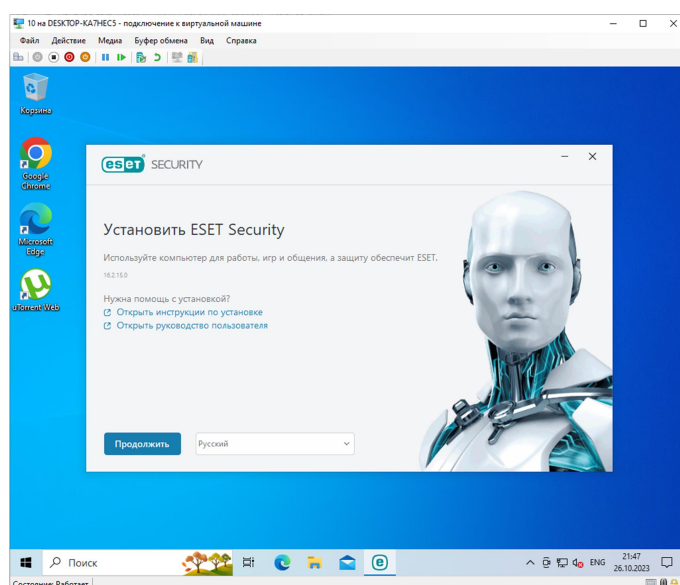


Рисунок 1

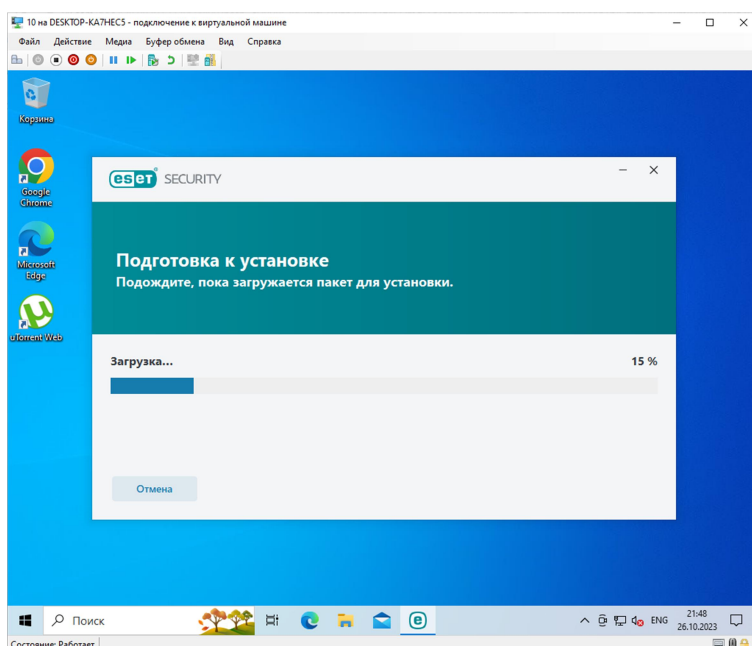


Рисунок 2

2. Выбираю указанные пункты и активирую пробную версию. Рисунок 3,4

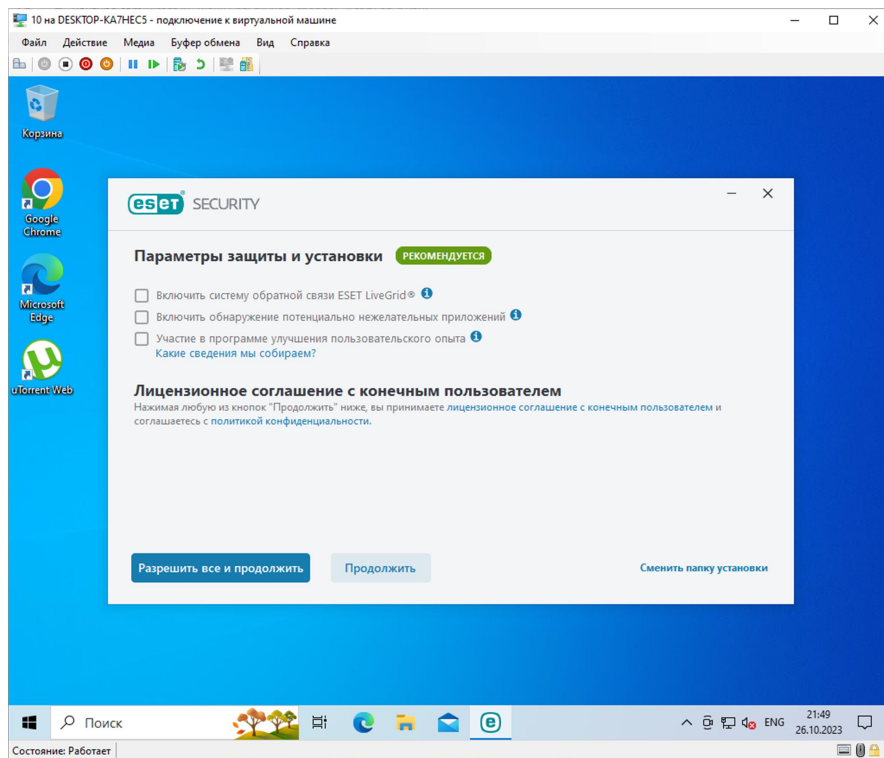


Рисунок 3

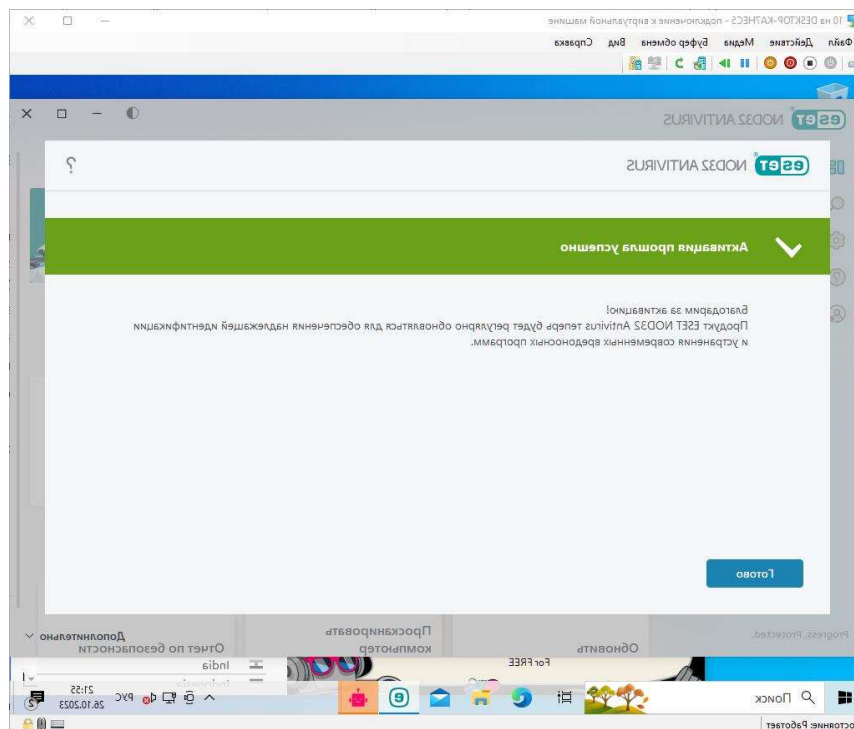


Рисунок 4

3. Произвожу настройку установленного ПО, согласно заданию. Рисунок 5,6.

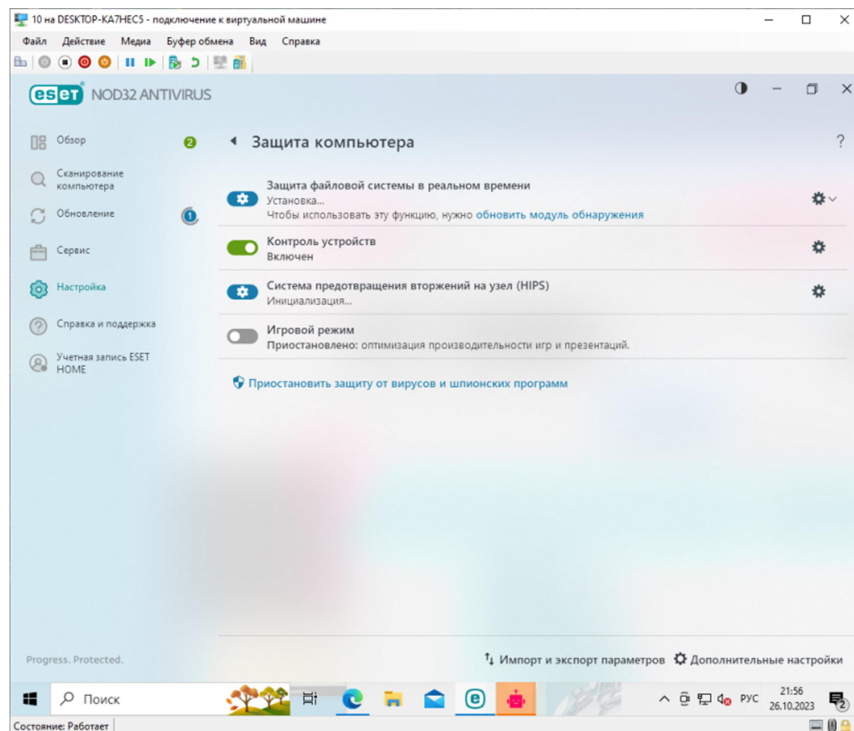


Рисунок 5

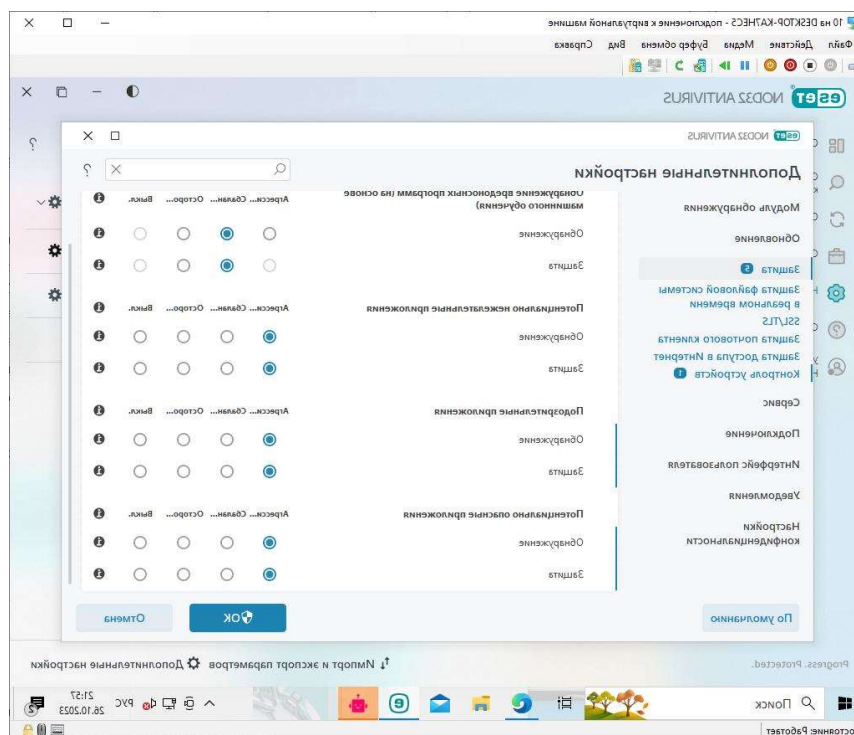


Рисунок 6

## ФОС для текущего контроля

### Задания для оценки знаний

1. Дайте определение понятию информационная безопасность.
2. Охарактеризуйте основные составляющие национальных интересов РФ в информационной сфере.
3. Охарактеризуйте угрозы информационной безопасности РФ.
4. Охарактеризуйте комплекс мер по совершенствованию информационной безопасности РФ.
5. Какие данные относятся к категории персональных?
6. Какая предусмотрена ответственность в РФ за ненадлежащее хранение персональных данных?
7. Дайте понятие метода обеспечения информационной безопасности.
8. Что является признаком компьютерного преступления?
9. В отношении каких сведений установлен режим защиты информации?
10. Проведите классификацию мер защиты информации
11. Перечислите основные характеристики надежного пароля?
12. Назовите системы или программы в которых вы создавали Пользователей?
13. Какие права доступа есть у Учетных записей пользователей Windows 7?
14. Что такое вирус?
15. Какие разновидности вирусов Вы знаете?
16. Как вирусы классифицируются по среде обитания?
17. Как вирусы классифицируются по степени вредного воздействия?
18. Какие виды вредоносных программ Вы знаете?
19. Как вирусы маскируются?
20. Когда обнаружили первый вирус?
21. Как Вы думаете, зачем изобретают вирусы?
22. Какие действия могут выполнять антивирусные программы?
23. Какие три задачи должна выполнять антивирусная программа?
24. Как обеспечить безопасность своей информации?

### Задания для оценки умений

1. Классифицируйте защищаемую информацию по видам тайны и степеням конфиденциальности.
2. Опишите меры по предотвращению угроз информационной безопасности для конкретной организации.

3. Проведите анализ типовых угроз при обработке информации в автоматизированных системах.
4. Сравните файловые, загрузочные и макровирусы, объясните их отличия.
5. Разработайте модель интеграции системы информационной безопасности в деятельность организации.
6. Опишите, как вы будете реагировать на попытку несанкционированного доступа к данным.
7. Проведите оценку рисков для выбранного информационного ресурса и предложите меры по их снижению
8. С помощью инструментов (например, *OWASP ZAP*, *Metasploit*, *Burp Suite*) найдите уязвимости в тестовом приложении.
9. Выполните шифрование файла с помощью *Cryptomator* или аналогичного инструмента.
10. Проанализируйте безопасность веб-приложения, выявите уязвимости сессий, *API* и внешних библиотек.
11. Дайте определение понятию «информационная безопасность».
12. Охарактеризуйте основные компоненты информационной безопасности.
13. Перечислите виды и источники угроз информационной безопасности.
14. Назовите основные законодательные акты и стандарты в области защиты информации в РФ.
15. Объясните, что такое «конфиденциальная информация» и приведите примеры её видов.

## Задания для самостоятельной работы

### Теоретические задания

1. Понятия информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем. Понятие «угроза информации».
4. Понятие «риск информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации.
6. Требования к системе защиты информации.
7. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
8. Целостность, доступность и конфиденциальность информации.
9. Классификация информации по видам тайны и степеням конфиденциальности. Понятие государственной тайны.
10. Понятие конфиденциальной информации. Виды конфиденциальной информации
11. Принципы засекречивания данных.
12. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
13. Цели и задачи защиты информации.
14. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации.
16. Понятие политики безопасности.
17. Понятие угрозы безопасности информации.
18. Системная классификация угроз безопасности информации. Каналы несанкционированного доступа к информации.
19. Методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
20. Анализ существующих методик определения требований к защите информации.
21. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
22. Виды мер и основные принципы защиты информации.
23. Организационная структура системы защиты информации. Законодательные акты в области защиты информации.
24. Российские и международные стандарты, определяющие требования к защите информации.
25. Система сертификации РФ в области защиты информации.

26. Основные правила системы сертификации РФ в области защиты информации.
27. Система защиты информации.
28. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
29. Программно-аппаратные средства защиты информации.
30. Инженерная защита объектов информатизации.
31. Техническая охрана объектов информатизации.
32. Принципы построения организационно-распорядительной системы. Доктрина информационной безопасности.
33. Классификация угроз информационной безопасности РФ по общей направленности.
34. Основные положения ФЗ «Об информации, информационных технологиях и защите информации».
35. Состав информации, необходимость защиты которой обусловлена интересами предприятия

### **Практические задания**

1. Создайте или найдите в сети Интернет и адаптируйте под свою организацию следующие документы:
  - 1.1 «Согласие на обработку персональных данных»
  - 1.2. «Согласие на обработку персональных данных (в случае получения данных у третьих лиц/передачи данных третьим лицам)»
  - 1.3. «Отзыв согласия на обработку персональных данных»
  - 1.4. «Журнал учета согласий субъектов персональных данных»
  - 1.5. «Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных»
  - 1.6. «Уведомление об обработке (о намерении осуществлять обработку) персональных данных», направляемое в Роскомнадзор.
  - 1.7. «Приказ о создании комиссии по проведению категорирования персональных данных и проведению инвентаризации/обследования информационных систем»
  - 1.8. «Опросный лист для сбора исходных данных об ИСПДн»
  - 1.9. «Акт категорирования персональных данных (перечень персональных данных)»
  - 1.10.«Перечень информационных систем»
  - 1.11.«Акт классификации информационной системы, обрабатывающей ПДн»
  - 1.12.«План мероприятий по защите персональных данных»
  - 1.13.«Положение о защите персональных данных»
  - 1.14.«Приказы о допуске»
  - 1.15.«Обязательство о неразглашении сведений персонального характера»
  - 1.16.«Журнал учета защищаемых носителей информации»
  - 1.17.«Акт на списание и уничтожение электронных носителей информации»