МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 15» Г. КАЛУГИ

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

1. [Вводные положения 4](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325410)

[1.1. Введение 4](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325411)

[1.2. Цели 4](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325412)

[1.3. Задачи 4](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325413)

[1.4. Область действия 5](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325414)

[1.5. Период действия и порядок внесения изменений 5](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325415)

[2. Термины и определения 5](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325416)

[3. Обозначения и сокращения 10](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325417)

[4. Политики информационной безопасности МБОУ «СОШ № 15». 10](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325418)

[4.1. Назначение политик информационной безопасности 10](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325419)

[4.2. Основные принципы обеспечения ИБ 11](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325420)

[4.3. Соответствие ПБ действующему законодательству 11](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325421)

[4.4. Ответственность за реализацию политик информационной безопасности 11](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325422)

[4.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе 11](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325423)

[4.6. Защищаемые информационные ресурсы МБОУ «СОШ № 15» 12](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325424)

[4.7. Организация системы управления информационной безопасностью МБОУ «СОШ № 103» 13](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325425)

[4.7.1. Организация системы управления ИБ 13](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325426)

[4.7.2. Реализация системы управления ИБ 14](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325427)

[4.7.3. Методы оценивания информационных рисков 14](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325428)

[4.8. Политики информационной безопасности 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325429)

[4.8.1. Политика предоставления доступа к информационному ресурсу 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325430)

[4.8.2. Назначение 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325431)

[4.8.2.1. Положение политики 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325432)

[4.8.3. Политика использования паролей 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325433)

[4.8.3.1. Назначение 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325434)

[4.8.3.2. Положения политики 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325435)

[4.8.4. Политика реализации антивирусной защиты 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325436)

[4.8.4.1. Назначение 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325437)

[4.8.4.2. Положения политики 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325438)

[4.8.5. Политика защиты АРМ 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325439)

[4.8.5.1. Назначение 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325440)

[4.8.5.2. Положения политики 15](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325441)

[4.9. Порядок сопровождения ИС МБОУ «СОШ № 15» 17](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325442)

[4.9.1. Профилактика нарушений политик информационной безопасности 18](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325443)

[4.9.2. Ликвидация последствий нарушения политик информационной безопасности 19](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325444)

[4.9.3. Ответственность нарушителей ПБ 19](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325445)

[5. Регулирующие законодательные нормативные документы 20](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325446)

[5.1. Основополагающие нормативные документы 20](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325447)

[5.2. Законы Российской Федерации 20](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325448)

[5.3. Указы и распоряжения президента Российской Федерации 22](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325449)

[5.4. Постановления и распоряжения правительства Российской Федерации 23](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325450)

[5.5. Нормативные и руководящие документы Федеральных служб РФ 23](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325451)

[5.6. Государственные стандарты 26](https://docviewer.yandex.ru/view/304526143/?*=TKhDtRAJtsIUcXHUKjSgta7WLIN7InVybCI6Imh0dHA6Ly9iYXJuLXNjaG9vbDEwMy51Y296LnJ1LzExMS8yMDE0LTIwMTUvcG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInRpdGxlIjoicG9saXRpa2FfaW5mb3JtYWNpb25ub2pfYmV6b3Bhc25vc3RpLmRvYyIsInVpZCI6IjMwNDUyNjE0MyIsInl1IjoiNzY2MTcyOTk2MTQ0NDAzNjY3NiIsIm5vaWZyYW1lIjp0cnVlLCJ0cyI6MTUwOTA5MzM5MzI5MX0%3D&lang=ru#_Toc404325452)

Вводные положения

1.1.​ Введение

Политика информационной безопасности разработана в соответствии с Федеральным законом от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 №152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002 №1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 06 марта 1997 №188 «Об утверждении Перечня сведений конфиденциального характера»,

Постановлением Правительства РФ No781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ No687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.

Политика информационной безопасности муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №15» г. Калуги (далее - МБОУ «СОШ № 15» г. Калуги) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется МБОУ «СОШ № 15» г. Калуги в своей деятельности.

Общее руководство обеспечением ИБ МБОУ «СОШ № 15» г. Калуги осуществляет директор школы. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ответственный за информатизацию (далее администратор информационной безопасности). Ответственность за функционирование автоматизированной системы учреждения несет инженер.

Должностные обязанности администратора информационной безопасности и инженера закрепляются в соответствующих инструкциях.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.2.​ Цели

Основными целями политики ИБ МБОУ «СОШ № 15» г. Калуги являются:

-сохранение конфиденциальности критичных информационных ресурсов;

-обеспечение непрерывности доступа к информационным ресурсам школы;

-защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;

-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;

-определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении.

-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;

-предотвращение и/или снижение ущерба от инцидентов ИБ.

1.3.​ Задачи

Политика информационной безопасности МБОУ «СОШ № 15» г. Калуги направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба МБОУ «СОШ № 15» г. Калуги обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне общества), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Для противодействия угрозам информационной безопасности в МБОУ «СОШ № 15» г. Калуги на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для МБОУ «СОШ № 15» г. Калуги. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

−​ описание организации системы управления информационной безопасностью в МБОУ «СОШ № 15» г. Калуги;

−​ определение Политик информационной безопасности МБОУ «СОШ № 15» г. Калуги, а именно:

−​ Политика реализации антивирусной защиты;

−​ Политика предоставления доступа к информационному ресурсу;

−​ Политика использования информационного ресурса в рамках существующих информационных систем;

−​ Политика использования паролей;

−​ Политика защиты АРМ;

−​ Политика конфиденциального делопроизводства;

−​ определение порядка сопровождения ИС МБОУ «СОШ № 15» г. Калуги.

1.4.​ Область действия

Настоящая Политика и обязательна для исполнения всеми сотрудниками и должностными лицами МБОУ «СОШ № 15» г. Калуги. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах МБОУ «СОШ № 15» г. Калуги, а также в договорах.

1.5.​ Период действия и порядок внесения изменений

Настоящая политика вводится в действие приказом руководителя учреждения.

Политика признается утратившей силу на основании приказа руководителя учреждения.

Изменения в политику вносятся приказом руководителя учреждения.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

−​ при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

−​ при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности МБОУ «СОШ № 15» г. Калуги;

−​ при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб МБОУ «СОШ № 15» г. Калуги.

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет заместитель директора по УВР, ответственный за защиту персональных данных, и инженер.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на заместителя директора по УВР, ответственный за защиту персональных данных, и инженер.

2.​ Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Инженер – специалист учреждения, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Администратор сети – сотрудник или группа сотрудников учреждения, которые выполняет функции администратора информационной безопасности, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

Актив – что-либо, что имеет ценность для учреждения.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим обществом (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Внутренняя сеть – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и DMZ межсетевым экраном. Внутренняя сеть объединяет производственные, тестовые, административные сети и сети разработчиков.

Демилитаризованная зона (DMZ) – участок корпоративной сети, расположенный между внешним МЭ и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет). В DMZ размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности не целесообразно размещать во внутренней сети МБОУ «СОШ № 15» г. Калуги.

Доступ к информации – возможность получения информации и ее использования.

Доступность – доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Доступность информации – состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов имеющих на это полномочия.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная среда – совокупность информационно-телекоммуникационной системы МБОУ «СОШ № 15» г. Калуги, процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных систем, обеспечивающего автоматизацию производственных процессов МБОУ «СОШ № 15» г. Калуги.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач подразделений МБОУ «СОШ № 15» г. Калуги. В МБОУ «СОШ № 15» г. Калуги используются различные типы информационных систем для решения производственных, управленческих, учетных и других задач.

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов МБОУ «СОШ № 15» г. Калуги, и средства защиты информации.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в производственных - процессах МБОУ «СОШ № 15» г. Калуги.

Инфраструктура открытых ключей (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Код аутентификации электронного сообщения – данные, используемые для установления подлинности и контроля целостности электронного сообщения.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Корпоративная сеть – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений МБОУ «СОШ № 15» г. Калуги, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений МБОУ «СОШ № 15» г. Калуги, привести к причинению МБОУ «СОШ № 15» г. Калуги материального или иного вида ущерба.

Криптопровайдер – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Менеджмент риска – скоординированные действия по руководству и управлению учреждением в отношении риска.

Мониторинг информационной безопасности – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы учреждения, информационные услуги учреждения и пр.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Остаточный риск – риск, остающийся после обработки риска.

Ответственное лицо (администратор) информационных активов – сотрудник МБОУ «СОШ № 15» г. Калуги, получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе Примечание: Понятия «Ответственное лицо (администратор) информационных активов» и «владелец информационных средств (ресурсов)» идентичны.

Оценивание риска – процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

Оценка риска – общий процесс анализа риска и оценивания риска.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник МБОУ «СОШ № 15» г. Калуги (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнесрисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Системный администратор – сотрудник учреждения, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Список контроля доступа (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля производства, разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Структурное подразделение – структурное подразделение учреждения с самостоятельными функциями, задачами и ответственностью.

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Удостоверяющий центр – автоматизированная система, включающая в себя аппаратно- программные средства, нормативно-методическую документацию и пользователей.

Узел – совокупность ЛВС МБОУ «СОШ № 15» г. Калуги, расположенных в пределах одной контролируемой зоны.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность – достоверность и полноту информации и методов ее обработки.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3.​ Обозначения и сокращения

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

ИОК – Инфраструктура открытых ключей.

ИС – Информационная система.

ИТС – Информационно-телекоммуникационная система.

КЗ – Контролируемая зона.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПО – Программное обеспечение.

СВТ – Средства вычислительной техники.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СПД – Система передачи данных.

СУБД – Система управления базами данных.

СУИБ – Система управления информационной безопасностью.

СЭД – Система электронного документооборота.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

ЭЦП – Электронная цифровая подпись.

4.​ Политики информационной безопасности МБОУ «СОШ № 103».

4.1.​ Назначение политик информационной безопасности

Политики информационной безопасности МБОУ «СОШ № 15» г. Калуги – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в МБОУ «СОШ № 15» г. Калуги.

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию МБОУ «СОШ № 15» г. Калуги в области ИБ.

Политики информационной безопасности (далее, ПБ) регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководителем учреждения.

4.2.​ Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

−​ Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.

−​ Своевременное обнаружение проблем, потенциально способных повлиять на ИБ общества, корректировка моделей угроз и нарушителя.

−​ Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей общества, а также повышать трудоемкость технологических процессов обработки информации.

−​ Контроль эффективности принимаемых защитных мер.

−​ Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4.3.​ Соответствие ПБ действующему законодательству

Правовую основу политик составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, МБОУ «СОШ № 15» г. Калуги и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

4.4.​ Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт заместитель директора по УВР, ответственный за защиту персональных данных, и инженер.

Ответственность за реализацию политик возлагается:

−​ в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на заместителя директора по УВР, ответственного за защиту персональных данных;

−​ в части, касающейся доведения правил политик до сотрудников МБОУ «СОШ № 15» г. Калуги, а также иных лиц (см. область действия настоящей политики) – на на заместителя директора по УВР, ответственного за защиту персональных данных;

−​ в части, касающейся исполнения правил политики, – на каждого сотрудника МБОУ «СОШ № 15» г. Калуги, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

4.5.​ Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников МБОУ «СОШ № 15» г. Калуги в области информационной безопасности возлагается на заместителя директора по УВР, ответственного за защиту персональных данных. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников МБОУ «СОШ № 15» г. Калуги правилам обращения с конфиденциальной информацией, проводится путем:

−​ проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в МБОУ «СОШ № 15» г. Калуги;

−​ самостоятельного изучения сотрудниками внутренних нормативных документов МБОУ «СОШ № 15» г. Калуги.

Допуск персонала к работе с информационными ресурсами МБОУ «СОШ № 15» г. Калуги осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в АС МБОУ «СОШ № 15» г. Калуги, а так же иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с конфиденциальной информацией МБОУ «СОШ № 15» г. Калуги осуществляется после ознакомления с «Инструкцией по обращению с носителями конфиденциальной информации». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками МБОУ «СОШ № 15» г. Калуги, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

4.6.​ Защищаемые информационные ресурсы МБОУ «СОШ № 15» г. Калуги

Различаются следующие категории информационных ресурсов, подлежащих защите в МБОУ «СОШ № 15» г. Калуги:

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности МБОУ «СОШ № 15» г. Калуги, которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности МБОУ «СОШ № 15» г. Калуги или имеющая принципиальное значение для имиджа МБОУ «СОШ № 15» г. Калуги;

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются «Инструкцией по обращению с носителями конфиденциальной информации», а также «Перечнем сведений конфиденциального характера».

Подходы к решению проблемы защиты информации в МБОУ «СОШ № 15» г. Калуги, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования производственных процессов МБОУ «СОШ № 15» г. Калуги.

Для этого в МБОУ «СОШ № 15» г. Калуги выполняются следующие мероприятия:

−​ определяется порядок работы с документами, образцами и др., содержащими конфиденциальные сведения;

−​ устанавливается круг лиц и порядок доступа к подобной информации;

−​ вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

−​ включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в МБОУ «СОШ № 15» г. Калуги. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых МБОУ «СОШ № 15» г. Калуги с другими организациями. Персональные данные сотрудника учреждения – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

−​ осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;

−​ разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4.7.​ Организация системы управления информационной безопасностью МБОУ «СОШ № 15» г. Калуги.

4.7.1.​ Организация системы управления ИБ

Система управления информационной безопасности МБОУ «СОШ № 15» г. Калуги (СУИБ) – предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности МБОУ «СОШ № 15» г. Калуги Для успешного функционирования СУИБ МБОУ «СОШ № 15» г. Калуги должны быть реализованы следующие процессы:

−​ определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

−​ определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью МБОУ «СОШ № 15» г. Калуги, а также оценки репутационных и правовых рисков деятельности МБОУ «СОШ № 15» г. Калуги;

−​ анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных процессов.

−​ выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

−​ принятие руководством МБОУ «СОШ № 15» г. Калуги остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности МБОУ «СОШ № 15» г. Калуги и оценено их влияние на достижение целей деятельности МБОУ «СОШ № 15» г. Калуги.

4.7.2.​ Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

−​ разработка плана обработки рисков ИБ;

−​ реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

−​ реализация программ по обучению и осведомленности ИБ;

−​ обнаружение и реагирование на инциденты безопасности;

−​ обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. МБОУ «СОШ № 15» г. Калуги принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

4.7.3.​ Методы оценивания информационных рисков

Оценка информационных рисков МБОУ «СОШ № 15» г. Калуги выполняется по следующим основным этапам:

−​ идентификация и количественная оценка информационных ресурсов, значимых для работы МБОУ «СОШ № 15» г. Калуги;

−​ оценивание возможных угроз;

−​ оценивание существующих уязвимостей;

−​ оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы МБОУ «СОШ № 15» г. Калуги подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

−​ показателей ценности информационных ресурсов;

−​ вероятности реализации угроз для ресурсов;

−​ эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса МБОУ «СОШ № 15» г. Калуги.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

−​ привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

−​ возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

−​ техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

−​ степенью легкости, с которой уязвимость может быть использована.

4.8.​ Политики информационной безопасности

4.8.1.​ Политика предоставления доступа к информационному ресурсу

4.8.2.​ Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам МБОУ «СОШ № 15» г. Калуги.

4.8.2.1.​ Положение политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

4.8.3.​ Политика использования паролей

4.8.3.1.​ Назначение

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к информационным активам МБОУ «СОШ № 15» г. Калуги.

4.8.3.2.​ Положения политики

Положения политики закрепляются в «Инструкции по парольной защите в АС».

4.8.4.​ Политика реализации антивирусной защиты

4.8.4.1.​ Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в МБОУ «СОШ № 15» г. Калуги.

4.8.4.2.​ Положения политики

Положения политики закрепляются в «Инструкции по проведению антивирусного контроля в АС».

4.8.5.​ Политика защиты АРМ

4.8.5.1.​ Назначение

Настоящая Политика определяет основные правила и требования по защите конфиденциальной информации МБОУ «СОШ № 15» г. Калуги от неавторизованного доступа, утраты или модификации.

4.8.5.2.​ Положения политики

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами предприятия, (согласно занимаемой должности), а именно: «Инструкция по обращению с носителями конфиденциальной информации», «Перечень сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено толькоинженер. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к инженеру, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом внедрения автоматизированных систем финансовых расчетов, и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками МБОУ «СОШ № 103». Запрещается использование указанных АРМ другими пользователями без согласования с начальником отдела внедрения автоматизированных систем финансовых расчетов. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка.

Инженер вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4.9.​ Порядок сопровождения ИС МБОУ «СОШ № 103»

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии инженера.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

−​ неверной формулировки требований к ИС;

−​ выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;

−​ принятия неверных проектных решений;

−​ внесения разработчиком дефектов на уровне архитектурных решений;

−​ внесения разработчиком недокументированных возможностей в ИС;

−​ неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;

−​ разработки некачественной документации;

−​ сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

−​ неверного конфигурирования ИС;

−​ приемки ИС, не отвечающей требованиям заказчика;

−​ внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство МБОУ «СОШ № 15» г. Калуги должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности производственного процесса.

−​ На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

−​ умышленное несанкционированное раскрытие, модификация или уничтожение информации;

−​ неумышленная модификация или уничтожение информации;

−​ недоставка или ошибочная доставка информации;

−​ отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

−​ внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

−​ невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб МБОУ «СОШ № 15» г. Калуги, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

4.9.1.​ Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в МБОУ «СОШ № 15» г. Калуги и проведение разъяснительной работы по информационной безопасности среди пользователей МБОУ «СОШ № 15» г. Калуги.

 Проведение в ИС МБОУ «СОШ № 15» г. Калуги регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС МБОУ «СОШ № 15» г. Калуги степенью периодичности.

Задача предупреждения в ИС МБОУ «СОШ № 15» г. Калуги возможных нарушений информационной безопасности решается по мере наступления следующих событий:

−​ включение в состав ИС МБОУ «СОШ № 15» г. Калуги новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС МБОУ «СОШ № 15» г. Калуги;

−​ изменение конфигурации программных и технических средств ИС МБОУ «СОШ № 15» г. Калуги (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС МБОУ «СОШ № 15» г. Калуги;

−​ при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС МБОУ «СОШ № 15» г. Калуги.

Администратор информационной безопасности (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС МБОУ «СОШ № 15» г. Калуги. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС МБОУ «СОШ № 15» г. Калуги путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС МБОУ «СОШ № 15» г. Калуги средств и функций защиты. По результатам профилактических работ, проводимых в ИС МБОУ «СОШ № 15» г. Калуги, необходимо сделать соответствующие записи в специальном журнале (Журнале проверки исправности и технического обслуживания).

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников МБОУ «СОШ № 15» г. Калуги по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в МБОУ «СОШ № 15» г. Калуги, проводится заместителем директора по УВР, ответственным за защиту персональных данных, ежеквартально.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников МБОУ «СОШ № 15» г. Калуги по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в МБОУ «СОШ № 15» г. Калуги, проводится при пересмотре настоящих политик, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

4.9.2.​ Ликвидация последствий нарушения политик информационной безопасности

Инженер, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС МБОУ «СОШ № 15» г. Калуги, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС МБОУ «СОШ № 15» г. Калуги рекомендуется уведомить инженера заместителя директора по УВР, ответственного за защиту персональных данных, и далее следовать их указаниям.

Действия инженера и заместителя директора по УВР, ответственного за защиту персональных данных, при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

−​ Инструкцией пользователя автоматизированной системы;

−​ Политикой информационной безопасности;

−​ Должностными обязанностями заместителя директора по УВР, ответственного за защиту персональных данных;

−​ Должностными обязанностями инженера.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС МБОУ «СОШ № 15» г. Калуги, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

4.9.3.​ Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник МБОУ «СОШ № 15» г. Калуги в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности МБОУ «СОШ № 15» г. Калуги, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный МБОУ «СОШ № 15» г. Калуги в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники МБОУ «СОШ № 15» г. Калуги несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники МБОУ «СОШ № 15» г. Калуги несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

5.​ Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники МБОУ «СОШ № 15» г. Калуги должны руководствоваться следующими законодательными нормативными документами:

5.1.​ Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

−​ Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);

−​ Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 1 июля 1994 г. № 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»);

−​ Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300, в редакции Указа Президента РФ от 10 января 2000 г. № 24);

−​ Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

5.2.​ Законы Российской Федерации

−​ Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности» (с изменениями от 25 декабря 1992 г., 24 декабря 1993 г., 25 июля 2002 г., 7 марта 2005 г., 25 июля 2006 г., 2 марта 2007 г.);

−​ Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ (с изменениями от 26 января, 20 февраля, 12 августа 1996 г., 24 октября 1997 г., 8 июля, 17 декабря 1999 г., 16 апреля, 15 мая, 26 ноября 2001 г., 21 марта, 14, 26 ноября 2002 г., 10 января, 26 марта, 11 ноября, 23 декабря 2003 г., 29 июня, 29 июля, 2, 29, 30 декабря 2004 г., 21 марта, 9 мая, 2, 18, 21 июля 2005 г., 3, 10 января, 2 февраля, 3, 30 июня, 27 июля, 3 ноября, 4, 18, 29, 30 декабря 2006 г., 26 января, 5 февраля, 20 апреля, 26 июня, 19, 24 июля, 2, 25 октября, 4, 29 ноября, 1, 6 декабря 2007 г.);

−​ Закон РоссийскойФедерации от 27 ноября 1992 г. № 4015-I «Об организации страхового дела в Российской Федерации» (с изменениями от 31 декабря 1997 г., 20 ноября 1999 г., 21 марта, 25 апреля 2002 г., 8, 10 декабря 2003 г., 21 июня, 20 июля 2004 г., 7 марта, 18, 21 июля 2005 г., 17 мая, 8, 29 ноября 2007 г.);

−​ Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности» (с изменениями от 22 августа 1995 г., 18 апреля 1996 г., 24 января 1998 г., 7 ноября, 27 декабря 2000 г., 6 августа, 30 декабря 2001 г., 25 июля 2002 г., 10 января 2003 г., 10 мая, 29 июня, 22 августа, 29 декабря 2004 г., 1 апреля, 9 мая 2005 г., 2 февраля, 25 октября, 4, 18 декабря 2006 г., 26 апреля, 18 октября 2007 г.);

−​ Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г., 29 июня, 22 августа 2004 г., 2 декабря 2005 г., 24 июля 2007 г.);

−​ Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (с изменениями от 8 ноября 2007 г.);

−​ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

−​ Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г.);

−​ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями от 23 декабря 2003 г., 22 августа, 2 ноября 2004 г., 9 мая 2005 г., 2 февраля, 3 марта, 26 июля, 29 декабря 2006 г., 9 февраля, 24 июля 2007 г.);

−​ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

−​ Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» (с изменениями от 30 декабря 1999 г., 7 ноября 2000 г., 30 декабря 2001 г., 7 мая, 25 июля 2002 г., 10 января, 30 июня 2003 г., 22 августа 2004 г., 7 марта 2005 г., 15 апреля, 27 июля 2006 г., 5, 24 июля, 4 декабря 2007 г.);

−​ Федеральный закон от 9 января 1996 г. № 2-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «О защите прав потребителей» и Кодекс РСФСР об административных правонарушениях» (с изменениями от 30 декабря 2001 г., 25 октября 2007 г.);

−​ Федеральный закон от 9 января 1996 г. № 3-ФЗ «О радиационной безопасности населения» (с изменениями от 22 августа 2004 г.);

−​ Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке» (с изменениями от 7 ноября 2000 г., 30 июня 2003 г., 22 августа 2004 г., 14 февраля 2007 г.);

−​ Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ (с изменениями от 27 мая, 25 июня 1998 г., 9 февраля, 15, 18 марта, 9 июля 1999 г., 9, 20 марта, 19 июня, 7 августа, 17 ноября, 29 декабря 2001 г., 4, 14 марта, 7 мая, 25 июня, 24, 25 июля, 31 октября 2002 г., 11 марта, 8 апреля, 4, 7 июля, 8 декабря 2003 г., 21, 26 июля, 28 декабря 2004 г., 21 июля, 19 декабря 2005 г., 5 января, 27 июля, 4, 30 декабря 2006 г., 9 апреля, 10 мая, 24 июля, 4 ноября, 1, 6 декабря 2007 г.);

−​ Федеральный закон от 13 декабря 1996 г. № 150-ФЗ «Об оружии» (с изменениями от 21, 31 июля, 17 декабря 1998 г., 19 ноября 1999 г., 10 апреля 2000 г., 26 июля, 8 августа, 27 ноября 2001 г., 25 июня, 25 июля 2002 г., 10 января, 30 июня, 8 декабря 2003 г., 26 апреля, 29 июня 2004 г., 18 июля, 29 декабря 2006 г., 24 июля 2007 г.);

−​ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);

−​ Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля, 31 декабря 2005 г., 27 июля, 4, 29 декабря 2006 г., 5 февраля, 19 июля, 4, 8 ноября, 1, 6 декабря 2007 г.).

5.3.​ Указы и распоряжения президента Российской Федерации

−​ Указ Президента Российской Федерации от 14 января 1992 г. № 20 «О защите государственных секретов Российской Федерации»;

−​ Указ Президента Российской Федерации от 7 октября 1993 г. № 1607 «О государственной политике в области охраны авторского права и смежных прав»;

−​ Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» (с изменениями от 17 января 1997 г., 1 сентября 2000 г.);

−​ Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);

−​ Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изменениями от 25 июля 2000 г.);

−​ Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации» (с изменениями от 16 августа 1995 г., 4 января 1996 г., 28 мая 1997 г., 29 ноября 2004 г.);

−​ Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г., 6 июня, 10 сентября 2001 г., 29 мая 2002 г., 3 марта 2005 г., 11 февраля 2006 г., 24 декабря 2007 г.);

−​ Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);

−​ Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» (с изменениями от 10 января 2000 г.);

−​ Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями от 22 марта, 20 июля 2005 г., 30 ноября 2006 г.);

−​ Указ Президента Российской Федерации от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»;

−​ Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.);

−​ Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» (с изменениями от 12 октября 2007 г.).

5.4.​ Постановления и распоряжения правительства Российской Федерации

−​ Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

−​ Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности» (с изменениями от 5 мая, 3 сентября, 2 октября 2007 г.);

−​ Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г., 26 января 2007 г.);

−​ Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

−​ Постановление Правительства РФ от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

−​ Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.);

−​ Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» (с изменениями от 15 января 2008 г.);

−​ Постановление Правительства Российской Федерацииот 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;

−​ Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» (с изменениями от 15 июля 2002 г.);

−​ Постановление Правительства Российской Федерации от 2 августа 1997 г. № 973 «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам»;

5.5.​ Нормативные и руководящие документы Федеральных служб РФ

−​ Решение Гостехкомиссии России от 21 октября 1997 г. № 61 «О защите информации при вхождении России в международную информационную систему «Интернет»;

−​ Приказ Федеральной службы по техническому и экспортному контролю от 28 августа 2007 г. № 181 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации»;

−​ Приказ ФСБ Российской Федерации от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

−​ Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР) (утверждено решением Гостехкомиссии России от 23 мая 1997 г. № 55-с);

−​ Постановление Госстандарта Российской Федерации от 21 сентября 1994 г. № 15 «Об утверждении «Порядка проведения сертификации продукции в Российской Федерации» (с изменениями от 25 июля 1996 г., 11 июля 2002 г.);

−​ Постановление Госстандарта Российской Федерации от 10 мая 2000 г. № 26 «Об утверждении Правил по проведению сертификации в Российской Федерации» (с изменениями от 5 июля 2002 г.);

−​ Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199);

−​ Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

−​ Положение об аккредитации испытательных лабораторийи органов по сертификации средств защиты информации по требованиям безопасности информации (утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

−​ Типовое положение об испытательной лаборатории (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 25 ноября 1994 г.);

−​ Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя

−​ Государственной технической комиссии при Президенте Российской Федерации т 5 января 1996 г. № 3);

−​ Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

−​ Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

−​ Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

−​ Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

−​ Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.);

−​ Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

−​ Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

−​ Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114);

−​ Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187);

−​ Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, Москва, 2002;

−​ Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, Москва, 2002;

−​ Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, Москва, 2002;

−​ Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах, Гостехкомиссия России, Москва, 2002;

−​ Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282);

−​ Приказ Минэнерго Российской Федерации от 13 января 2003 г. № 6 «Об утверждении Правил технической эксплуатации электроустановок потребителей»;

−​ Приказ Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст «О введении в действие межгосударственных стандартов»;

−​ Руководящий документ РД 50-082-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения», 1989 г.;

−​ Руководящий документ РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов», 1990 г.;

−​ Руководящий документ РД 50-680-88 «Методические указания. Автоматизированные системы. Основные положения», 1988 г.;

−​ Рекомендация Р 50-34.119-90 «Рекомендации. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Архитектура локальных вычислительных сетей в системах промышленной автоматизации. Общие положения», 1990 г.;

−​ Рекомендация Р 50.4.002-2000 «Рекомендации по аккредитации. Инспекционный контроль за деятельностью в системе сертификации», 2000 г.;

−​ Рекомендация МИ 2377-98 «Рекомендация. Государственная система обеспечения единства измерений. Разработка и аттестация методик выполнения измерений», 1998 г.;

−​ Методические указания МИ 1317-86 «Методические указания. Государственная система обеспечения единства измерений. Результаты и характеристики погрешности измерений. Формы представления. Способы использования при испытаниях образцов продукции и контроля их параметров», 1986 г.;

−​ Строительные нормы и правила СНиП 23-03-2003 «Защита от шума» (введены в ействие постановлением Госстроя РФ от 30 июня 2003 г. № 136);

−​ Письмо Министерства промышленности и энергетики Российской Федерации и Министерства регионального развития Российской Федерации от 29 ноября 2006 г. № АР-6893/08, 12325-ЮТ/08;

−​ Постановление Главного государственного санитарного врача Российской Федерации от 3 июня 2003 г. № 118 «О введении в действие санитарно- эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» (с изменениями от 25 апреля 2007 г.);

−​ Нормы пожарной безопасности НПБ 88-2001 «Установки пожаротушения и сигнализации. Нормы и правила проектирования» (утверждены приказом ГУГПС МВД РФ от 4 июня 2001 г. N 31, с изменениями от 31 декабря 2002 г.);

−​ Строительные нормы и правила СНиП 2.01.15-90 «Инженерная защита территорий, зданий и сооружений от опасных геологических процессов. Основные положения проектирования» (утверждены постановлением Госстроя СССР от 29 декабря 1990 г. № 118);

−​ Строительные нормы и правила СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование» (приняты постановлением Госстроя РФ от 26 июня 2003 г. № 115);

−​ Строительные нормы и правила СНиП 21-01-97 «Пожарная безопасность зданий и сооружений» (утверждены постановлением Минстроя РФ от 13 февраля 1997 г. № 18-7, с изменениями от 3 июня 1999 г., 19 июля 2002 г.).

5.6.​ Государственные стандарты

−​ ГОСТ 2.051-2006 «Единая система конструкторской документации. Электронные документы. Общие положения» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 119-ст);

−​ ГОСТ 2.101-68 «Единая система конструкторской документации. Виды изделий» (утвержден Госстандартом СССР в декабре 1967 г.);

−​ ГОСТ 2.102-68 «Единая система конструкторской документации. Виды и комплектность конструкторских документов» (утвержден постановлением Госстандарта СССР от 28 июня 1968 г. № 1029, изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.103-68 «Единая система конструкторской документации. Стадии разработки» (введен в действие Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 118-ст);

−​ ГОСТ 2.111-68 «Единая система конструкторской документации. Нормоконтроль» (утвержден Госстандартом СССР в декабре 1967 г., с изменениями от 22 июня 2006 г.);

−​ ГОСТ 18321-73 «Статистический контроль качества. Методы случайного отбора выборок штучной продукции» (введен в действие постановлением Государственного комитета стандартов Совета Министров СССР от 9 января 1973 г. № 33);

−​ ГОСТ 2.109-73 «Единая система конструкторской документации. Основные требования к чертежам» (утвержден постановлением Госстандарта СССР от 27 июля 1973 г. № 1843, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.118-73 «Единая система конструкторской документации. Техническое предложение» (введен постановлением Госстандарта СССР от 28 февраля 1973 г. № 500, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.119-73 «Единая система конструкторской документации. Эскизный проект» (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 501, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.120-73 «Единая система конструкторской документации. Технический проект» (введен в действие постановлением Госстандарта СССР от 28 февраля 1973 г. № 502, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 19.001-77 «Единая система программной документации. Общие положения» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);

−​ ГОСТ 19.101-77 «Единая система программной документации. Виды программ и программных документов» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268, с изменениями от июня 1981 г.);

−​ ГОСТ 19.102-77 «Единая система программной документации. Стадии разработки» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);

−​ ГОСТ 19.103-77 «Единая система программной документации. Обозначения программ и программных документов» (введен в действие постановлением Госстандарта СССР от 20 мая 1977 г. № 1268);

−​ ГОСТ Р 50779.10-2000 (ИСО 3534.1-93) «Статистические методы. Вероятность и основы статистики. Термины и определения» (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);

−​ ГОСТ Р 50779.11-2000 (ИСО 3534.2-93) «Статистические методы. Статистическое управление качеством. Термины и определения» (введен в действие постановлением Госстандарта России от 29 декабря 2000 N 429-ст);

−​ ГОСТ 19.104-78 «Единая система программной документации. Основные надписи» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.105-78 «Единая система программной документации. Общие требования к программным документам» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.106-78 «Единая система программной документации. Требования к программным документам, выполненным печатным способом» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.201-78 (СТ СЭВ 1627-79) «Единая система программной документации. Техническое задание. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от июля 1981 г.);

−​ ГОСТ 19.202-78 (СТ СЭВ 2090-80) «Единая система программной документации. Спецификация. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.401-78 «Единая система программной документации. Текст программы. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от июля 1982 г.);

−​ ГОСТ 19.402-78 «Единая система программной документации. Описание программы» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.501-78 «Единая система программной документации. Формуляр. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3351);

−​ \_ ГОСТ 19.502-78 «Единая система программной документации. Описание применения. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 18 декабря 1978 г. № 3350, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.601-78 «Единая система программной документации. Общие правила дублирования, учета и хранения» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);

−​ ГОСТ 19.602-78 «Единая система программной документации. Правила дублирования, учета и хранения программных документов, выполненных печатным способом» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518);

−​ ГОСТ 19.603-78 «Единая система программной документации. Общие правила внесения изменений» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.604-78 «Единая система программной документации. Правила внесения изменений в программные документы, выполненные печатным способом» (введен в действие постановлением Госстандарта СССР от 22 февраля 1978 г. № 518, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.403-79 «Единая система программной документации. Ведомость держателей подлинников» (введен в действие постановлением Госстандарта СССР от 28 июня 1979 г. № 2335);

−​ ГОСТ 19.404-79 «Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753);

−​ ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753, с изменениями от февраля 1982 г.);

−​ ГОСТ 19.503-79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.504-79 «Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.505-79 «Единая система программной документации. Руководство ператора. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.506-79 «Единая система программной документации. Описание языка. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 12 января 1979 г. № 74, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.507-79 «Единая система программной документации. Ведомость эксплуатационных документов» (введен в действие постановлением Госстандарта СССР от 28 июня 1979 г. № 2335, с изменениями от сентября 1981 г.);

−​ ГОСТ 19.508-79 «Единая система программной документации. Руководство по техническому обслуживанию. Требования к содержанию и оформлению» (введен в действие постановлением Госстандарта СССР от 11 декабря 1979 г. № 4753);

−​ ГОСТ 17168-82 (СТ СЭВ 1807-79) «Фильтры электронные октавные и третьоктавные. Общие технические требования и методы испытаний» (введен в действие постановлением Госстандарта СССР от 29 марта 1979 г. № 1294);

−​ ГОСТ 12.1.003-83 (СТ СЭВ 1930-79) «Система стандартов безопасности труда. Шум. Общие требования безопасности» (утвержден постановлением Госстандарта СССР от 6 июня 1983 г. № 2473, с изменениями от 19 декабря 1988 г.);

−​ ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение» (утвержден постановлением Госстандарта СССР от 28 июня 1984 г. № 2206, с изменениями от июня 1987 г., ноября 1988 г., декабря 1990 г.);

−​ ГОСТ 2.701-84 «Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению» (утвержден постановлением Госстандарта СССР от 29 августа 1984 г. № 3038);

−​ ГОСТ 2.124-85 «Единая система конструкторской документации. Порядок применения покупных изделий» (введен в действие постановлением Госстандарта СССР от 13 декабря 1984 г. № 123);

−​ ГОСТ 12.1.050-86 «Система стандартов безопасности труда. Методы измерения шума на рабочих местах» (введен в действие постановлением Госстандарта СССР от 28 марта 1986 г. № 790, с изменениями от 31 мая 2005 г.);

−​ ГОСТ 27296-87 (СТ СЭВ 4866-84) «Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Методы измерения» (введен в действие постановлением Госстроя СССР от 11 сентября 1985 г. № 145);

−​ ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования» (утвержден постановлением Госстандарта СССР от 28 января 1987 г. № 124, с изменениями от 24 марта 1989 г., 26 декабря 1990 г.);

−​ ГОСТ 2.004-88 «Единая система конструкторской документации. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ» (утвержден постановлением Госстандарта СССР от 28 ноября 1988 г. № 3843);

−​ ГОСТ 2.125-88 «Единая система конструкторской документации. Правила выполнения эскизных конструкторских документов» (утвержден постановлением Госстандарта СССР от 22 июля 1988 г. № 2714);

−​ ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем» (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 664, с изменениями от 29 декабря 1990 г.);

−​ ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы"(утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);

−​ ГОСТ 28195-89 «Оценка качества программных средств. Общие положения» (утвержден постановлением Госстандарта СССР от 28 июля 1989 г. № 2507);

−​ ГОСТ 28388-89 «Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 20 декабря 1989 г. № 3903);

−​ ГОСТ 28806-90 «Качество программных средств. Термины и определения» (утвержден постановлением Госстандарта СССР от 25 декабря 1990 г. № 3278);

−​ ГОСТ 19.701-90 (ИСО 5807-85) «Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 декабря 1990 г. № 3294);

−​ ГОСТ 19781-90 «Единая система программной документации. Обеспечение систем обработки информации программное. Термины и определения» (введен в действие постановлением Госстандарта СССР от 27 августа 1990 г. № 2467);

−​ ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утвержден постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399);

−​ ГОСТ 2.503-90 «Единая система конструкторской документации. Правила внесения изменений» (утвержден постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 апреля 1990 г. № 1031, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания» (утвержден постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469);

−​ ГОСТ 22505-97 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний» (утвержден постановлением Госстандарта России от 28 августа 1998 г. № 337);

−​ ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем» (утвержден постановлением Комитета стандартизации и метрологии СССР от 17 февраля 1992 г. № 161);

−​ ГОСТ Р ИСО/МЭК ТО 9294-93 «Информационная технология. Руководство по управлению документированием программного обеспечения» (утвержденпостановлением Госстандарта России от 20 декабря 1993 г. № 260);

−​ ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению» (утвержден постановлением Госстандарта России от 28 декабря 1993 г. № 267);

−​ ГОСТ 2.001-93 «Единая система конструкторской документации. Общие положения» (введен в действие постановлением Госстандарта России от 3 марта 1994 г. № 50, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.123-93 «Единая система конструкторской документации. Комплектность конструкторских документов на печатные платы при автоматизированном проектировании» (введен в действие постановлением Госстандарта России от 2 марта 1994 г. № 44);

−​ ГОСТ Р ИСО 9127-94 «Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов» (принят постановлением Госстандарта России от 10 октября 1994 г. № 242);

−​ ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (принят постановлением Госстандарта России от 15 мая 1996 г. № 308);

−​ ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);

−​ ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний», Госстандарт России, 1995 г.;

−​ ГОСТ 2.105-95 «Единая система конструкторскойдокументации. Общие требования к текстовым документам» (введен в действие постановлением Госстандарта России от 8 августа 1995 г. № 426, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.602-95 «Единая система конструкторской документации. Ремонтные документы» (введен в действие постановлением Госстандарта России от 29 февраля 1996 г. № 131, с изменениями от 22 июня 2006 г.);

−​ ГОСТ 2.106-96 «Единая система конструкторской документации. Текстовые документы» (введен в действие постановлением Госстандарта России от 13 ноября 1996 г. № 620, с изменениями от 22 июня 2006 г.);

−​ ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 450);

−​ ГОСТ Р ИСО 9001-2001 «Системы менеджмента качества. Требования» (утвержден постановлением Госстандарта России от 15 августа 2001 г. № 333-ст, с изменениями от 7 июля 2003 г.);

−​ ГОСТ 2.780-96 «Единая система конструкторской документации. Обозначения условные графические. Кондиционеры рабочей среды, емкости гидравлические и пневматические» (утвержден постановлением Госстандарта РФ от 7 апреля 1997 г. № 121);

−​ ГОСТ 2.784-96 «Единая система конструкторской документации. Обозначения условные графические. Элементы трубопроводов» (введен в действие постановлением Госстандарта России от 7 апреля 1997 г. № 124);

−​ ГОСТ Р 50923-96 «Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения» (введен в действие постановлением Госстандарта России от 10 июля 1996 г. № 451);

−​ ГОСТ 22505-97 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний» (введен в действие постановлением Госстандарта России от 28 августа 1998 г. № 337);

−​ ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);

−​ ГОСТ Р 51171-98 «Качество служебной информации. Правила предъявления информационных технологий на сертификацию» (введен в действие постановлением Госстандарта России от 12 мая 1998 г. № 184);

−​ ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);

−​ ГОСТ Р ИСО/МЭК 12207-99 «Информационная технология. Процессы жизненного цикла программных средств» (принят и введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 675-ст);

−​ ГОСТ Р 51320-99 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех» (введен в действие постановлением Госстандарта России от 22 декабря 1999 г. № 655-ст);

−​ ГОСТ Р 50779.72-99 (ИСО 2859-2-85) «Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 2. Планы выборочного контроля отдельных партий на основе предельного качества LQ» (введен в действие постановлением Госстандарта России от 23 декабря 1999 г. № 694-ст);

−​ ГОСТ Р 51319-99 «Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний» (введен в действие постановлением Госстандарта России от 28 декабря 1999 г. № 795-ст);

−​ ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», Госстандарт России, 2000 г.;

−​ ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования», Госстандарт России, 2000 г.;

−​ ГОСТ Р ИСО/МЭК 17025-2006 «Общие требования к компетентности испытательных и калибровочных лабораторий» (введен в действие постановлением Госстандарта России от 27 декабря 2006 г. № 506-ст);

−​ ГОСТ Р 40.002-2000 «Система сертификации ГОСТ Р. Регистр систем качества. Основные положения» (принят постановлением Госстандарта РФ от 13 апреля

−​ 2000 г. № 107-ст);

−​ ГОСТ Р ИСО/МЭК 65-2000 «Общие требования к органам по сертификации продукции» (утвержден постановлением Госстандарта РФ от 7 апреля 2000 г. № 96-ст);

−​ ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний» (введен в действие постановлением Госстандарта России от 26 декабря 2000 г. № 417-ст);

−​ ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь»(принят постановлением Госстандарта России от 15 августа 2001 г. № 332-ст, с изменениями от 7 июля 2003 г.);

−​ ГОСТ Р ИСО 9004-2001 «Системы менеджмента качества. Рекомендации по улучшению деятельности» (принят постановлением Госстандарта России от 15 августа 2001 г. № 334-ст, с изменениями от 7 июля 2003 г.);

−​ ГОСТ Р 50948-2001 «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности» (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);

−​ ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности» (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст);

−​ ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);

−​ ГОСТ Р ИСО/МЭК 15408-2-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности» (принят постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);

−​ ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» (принят и введен в действие постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст);

−​ ГОСТ Р 40.003-2005 «Система сертификации ГОСТ Р. Регистр систем качества. Порядок сертификации систем менеджмента качества на соответствие ГОСТ Р ИСО 9001-2001 (ИСО 9001:2000)» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 14 ноября 2005 г. № 287-ст);

−​ ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст);

1.4.

Выполнение требований Политики ИБ является обязательным

для всех структурных подразделений школы.

1.5.

Ответственность за соблюдение информационной безопасности

несет каждый сотрудник школы. На лиц, работающих в управлении по

договорам гражданско-правового характера, положения настоящей

политики распространяются в случае, если это обусловлено в таком

договоре.

2. Цель и задачи политики информационной безопасности.

2.1.

Основными задачами политики ИБ являются:

-разработка требований по обеспечению ИБ;

-контроль выполнения установленных требований по обеспечению ИБ;

повышениеэффективности,непрерывности,контролируемостимероприятий по

обеспечению и поддержанию ИБ;

-разработка нормативных документов для обеспечения ИБ школы;

-выявление, оценка, прогнозирование и предотвращение реализации угроз

ИБ школы;

-организация антивирусной защиты информационных ресурсов школы;

-защита информации школы от несанкционированного доступа (далее-НСД)

и утечки по техническим каналам связи;

-организация периодической проверки соблюдения информационной

безопасности с последующим представлением отчета по результатам

указанной проверки директору школы.

3. Концептуальная схема обеспечения информационной безопасности.

3.1.

Политика ИБ школы направлена на защиту информационных

ресурсов (активов) от угроз, исходящих от противоправных действий

злоумышленников, уменьшение рисков и снижение потенциального

вреда от аварий, непреднамеренных ошибочных действий сотрудников

школы, технических сбоев автоматизированных систем, неправильных

технологических и организационных решений в процессах поиска,

сбора хранения, обработки, предоставления и распространения

информации и обеспечение эффективного и бесперебойного процесса

деятельности.

3.2.

Наибольшими возможностями для нанесения ущерба обладает

собственный персонал школы. Риск аварий и технических сбоев в

автоматизированных системах определяется состоянием аппаратного

обеспечения, надежностью систем энергоснабжения и

телекоммуникаций, квалификацией сотрудников и их способностью к

адекватным и незамедлительным действиям в нештатной ситуации.

3.3.

Стратегия обеспечения ИБ школы заключается в использовании

заранее разработанных мер противодействия атакам злоумышленников,

а также программно- технических и организационных решений,

позволяющих свести к минимуму возможные потери от технических

аварий и ошибочных действий сотрудников школы.

4. Основные принципы обеспечения информационной безопасности.

4.1.

Основными принципами обеспечения ИБ:

-постоянный и всесторонний анализ автоматизированных систем и трудового

процесса с целью выявления уязвимости информационных активов школы;

-своевременное обнаружение проблем, потенциально способных повлиять на

ИБ школы, корректировка моделей угроз и нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

-персонификация и разделение ролей и ответственности между сотрудниками

школы за обеспечение ИБ школы исходит из принципа персональной и

единоличной ответственности за совершаемые операции.

5.Объекты защиты.

5.1.

Объектами защиты с точки зрения ИБ в управлении являются:

-информационный процесс профессиональной деятельности;

-информационные активы школы.

5.2.

Защищаемая информация делится на следующие виды:

-информация по финансово-экономической деятельности школы;

-персональные данные – любая информация, относящаяся к определенному

или определяемому на основании такой информации физическому лицу

(субъекту персональных данных), в том числе его фамилия, имя, отчество,

год, месяц, дата и место рождения, адрес, семейное, социальное,

имущественное положение, образование,

профессия, доходы, другая информация;

-другая информация, не относящаяся ни к одному из указанных выше видов,

которая отмечена грифом «Для служебного пользования» или

«Конфиденциально».

6. Требования по информационной безопасности.

6.1.

В отношении всех собственных информационных активов школы,

активов, находящихся под контролем школы, а также активов,

используемых для получения доступа к инфраструктуре школы, должна

быть определена ответственность соответствующего сотрудника

школы. Информация о смене владельцев активов, их распределении,

изменениях в конфигурации и использовании за пределами школы

должна доводиться до сведения начальника школы.

6.2.

Все работы в пределах школы должны выполняться в

соответствии с официальными должностными обязанностями только на

компьютерах, разрешенных к использованию в управлении.

6.3.

Внос в здание и помещения школы личных портативных

компьютеров и внешних носителей информации (диски, дискеты,

флэш-карты и т.п.), а также вынос их за пределы школы производится

только при согласовании с администратором ЛВС.

6.4.

Все данные (конфиденциальные или строго конфиденциальные),

составляющие тайну школы и хранящиеся на жестких дисках

портативных компьютеров, должны быть зашифрованы.

6.5.

Руководители подразделений должны периодически

пересматривать права доступа своих сотрудников и других

пользователей к соответствующим информационным ресурсам.

6.6.

В целях обеспечения санкционированного доступа к

информационному ресурсу, любой вход в систему должен

осуществляться с использованием уникального имени пользователя и

пароля.

6.7.

Пользователи должны руководствоваться рекомендациями по

защите своего пароля на этапе его выбора и последующего

использования. Запрещается сообщать свой пароль другим лицам или

предоставлять свою учетную запись другим, в том числе членам своей

семьи и близким.

6.8.

В процессе своей работы сотрудники обязаны постоянно

использовать режим "Экранной заставки" с парольной защитой.

Рекомендуется устанавливать максимальное время "простоя"

компьютера до появления экранной заставки не дольше 15 минут.

6.9.

Каждый сотрудник обязан немедленно уведомить администратора

ЛВС обо всех случаях предоставления доступа третьим лицам к

ресурсам корпоративной сети. Доступ третьих лиц к информационным

системам школы должен быть обусловлен производственной

необходимостью. В связи с этим, порядок доступа к информационным

ресурсам школы должен быть четко определен, контролируем и

защищен.

6.10.

Сотрудникам, использующим в работе портативные компьютеры

школы, может быть предоставлен удаленный доступ к сетевым

ресурсам школы в соответствии с правами в корпоративной

информационной системе.

6.11.

Сотрудникам, работающим за пределами школы с

использованием компьютера, не принадлежащего управлению,

запрещено копирование данных на компьютер, с которого

осуществляется удаленный доступ.

6.12.

Сотрудники, имеющие право удаленного доступа к

информационным ресурсам школы, должны соблюдать требование,

исключающее одновременное подключение их компьютера к сети

школы и к каким-либо другим сетям, не принадлежащим школы.

6.13.

Все компьютеры, подключаемые посредством удаленного доступа

к информационной сети школы, должны иметь программное

обеспечение антивирусной защиты, имеющее последние обновления.

Доступ к сети Интернет обеспечивается только в производственных

целях и не может использоваться для незаконной деятельности.

6.14.

Рекомендованные правила:

-сотрудникам школы разрешается использовать сеть Интернет только в

служебных целях;

-запрещается посещение любого сайта в сети Интернет, который считается

оскорбительным для общественного мнения или содержит информацию

сексуального характера, пропаганду расовой ненависти, комментарии по

поводу различия/превосходства полов, дискредитирующие заявления или

иные материалы с оскорбительными высказываниями по поводу чьего-либо

возраста, сексуальной

ориентации, религиозных или политических убеждений, национального

происхождения или недееспособности;

-сотрудники школы не должны использовать сеть Интернет для хранения

корпоративных данных;

-работа сотрудников школы с Интернет-ресурсами допускается только

режимом просмотра информации, исключая возможность передачи

информации школы в сеть Интернет;

-сотрудникам, имеющим личные учетные записи, предоставленные

публичными провайдерами, не разрешается пользоваться ими на

оборудовании, принадлежащем управлению;

-сотрудники школы перед открытием или распространением файлов,

полученных через сеть Интернет, должны проверить их на наличие вирусов;

-запрещен доступ в Интернет через сеть школы для всех лиц, не являющихся

сотрудниками школы, включая членов семьи сотрудников школы.

6.15.

Администратор ЛВС имеет право контролировать содержание

всего потока

информации, проходящей через канал связи к сети Интернет в обоих

направлениях

6.16.

Сотрудники должны постоянно помнить о необходимости

обеспечения физической безопасности оборудования, на котором

хранится информация школы.

6.17.

Сотрудникам запрещено самостоятельно изменять конфигурацию

аппаратного и программного обеспечения. Все изменения производит

администратор ЛВС.

6.18.

Все компьютерное оборудование (серверы, стационарные и

портативные компьютеры), периферийное оборудование (например,

принтеры и сканеры), аксессуары (манипуляторы типа "мышь",

шаровые манипуляторы, дисководы для С

D

-дисков),

коммуникационное оборудование (например, факс-модемы, сетевые

адаптеры и концентраторы), для целей настоящей политики вместе

именуются "компьютерное оборудование". Компьютерное

оборудование, предоставленное управлением, является ее

собственностью и предназначено для использования исключительно в

производственных целях.

6.19.

Каждый сотрудник, получивший в пользование портативный

компьютер, обязан принять надлежащие меры по обеспечению его

сохранности.

6.20.

Все компьютеры должны защищаться паролем при загрузке

системы, активации по горячей клавиши и после выхода из режима

"Экранной заставки". Для установки режимов защиты пользователь

должен обратиться к администратору ЛВС. Данные не должны быть

скомпрометированы в случае халатности или небрежности приведшей

к потере оборудования. Перед утилизацией все компоненты

оборудования, в состав которых входят носители данных (включая

жесткие диски), необходимо проверять, чтобы убедиться в отсутствии

на них конфиденциальных данных и лицензионных продуктов. Должна

выполняться процедура форматирования носителей информации,

исключающая возможность восстановления данных.

6.21.

Порты передачи данных, в том числе

FDD

и

CD

дисководы в

стационарных компьютерах сотрудников школы блокируются, за

исключением тех случаев, когда сотрудником получено разрешение на

запись администратора ЛВС.

6.22.

Все программное обеспечение, установленное на

предоставленном управлением компьютерном оборудовании, является

собственностью школы и должно использоваться исключительно в

производственных целях.

6.23.

Сотрудникам запрещается устанавливать на предоставленном в

пользование компьютерном оборудовании нестандартное,

нелицензионное программное обеспечение или программное

обеспечение, не имеющее отношения к их производственной

деятельности.

6.24.

На всех портативных компьютерах должны быть установлены

программы,необходимые для обеспечения защиты информации:

- персональный межсетевой экран;

- антивирусное программное обеспечение;

- программное обеспечение шифрования жестких дисков;

- программное обеспечение шифрования почтовых сообщений

6.25.

Все компьютеры, подключенные к корпоративной сети, должны

быть оснащены системой антивирусной защиты, утвержденной

администратором ЛВС.

6.26.

Сотрудники школы не должны:

- блокировать антивирусное программное обеспечение;

- устанавливать другое антивирусное программное обеспечение;

- изменять настройки и конфигурацию антивирусного программного

обеспечения.

6.27.

Электронные сообщения должны строго соответствовать

стандартам в области деловой этики. Использование электронной

почты в личных целях не допускается. Сотрудникам запрещается

направлять конфиденциальную информацию школы по электронной

почте без использования систем шифрования. Строго

конфиденциальная информация школы, ни при каких обстоятельствах,

не подлежит пересылке третьим лицам по электронной почте.

6.28.

Использование сотрудниками школы публичных почтовых

ящиков электронной почты осуществляется только при согласовании с

ответственным за обеспечение безопасности информации ЛВС при

условии применения механизмов шифрования.

6.29.

Сотрудники школы для обмена документами должны

использовать только свой официальный адрес электронной почты.

6.30.

Сообщения, пересылаемые по электронной почте, представляют

собой постоянно используемый инструмент для электронных

коммуникаций, имеющих тот же статус, что и письма и факсимильные

сообщения. Электронные сообщения подлежат такому же утверждению

и хранению, что и прочие средства письменных коммуникаций. В целях

предотвращения ошибок при отправке сообщений пользователи перед

отправкой должны внимательно проверить правильность написания

имен и адресов получателей. В случае получения сообщения лицом,

вниманию которого это сообщение не предназначается, такое

сообщение необходимо переправить непосредственному получателю.

Если полученная таким образом информация носит конфиденциальный

характер, об этом следует незамедлительно проинформировать

администратора ЛВС. Отправитель электронного сообщения,

документа или лицо, которое его переадресовывает, должен указать

свое имя и фамилию, служебный адрес и тему сообщения.

6.31.

Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные

ресурсы электронной почты;

- рассылка рекламных материалов;

- подписка на рассылку, участие в дискуссиях и подобные услуги,

использующие значительные ресурсы электронной почты в личных целях;

- поиск и чтение сообщений, направленных другим лицам (независимо от

способа их хранения);

- пересылка любых материалов, как сообщений, так и приложений,

содержание которых

вляетсяпротивозаконным,непристойным,злонамеренным,оскорбительным,

угрожающим, клеветническим, злобным или способствует поведению,

которое может рассматриваться как уголовное преступление или

административный проступок либо приводит к возникновению гражданско-

правовой ответственности, беспорядков или противоречит стандартам в

области этики.

6.32.

Объем пересылаемого сообщения по электронной почте не

должен превышать 2 Мбайт.

6.33.

Все пользователи должны быть осведомлены о своей обязанности

сообщать об известных или подозреваемых ими нарушениях

информационной безопасности, а также должны быть

проинформированы о том, что ни при каких обстоятельствах они не

должны пытаться использовать ставшие им известными слабые

стороны системы безопасности.

6.34.

В случае кражи переносного компьютера следует

незамедлительно сообщить администратору ЛВС.

6.35.

Если имеется подозрение или выявлено наличие вирусов или

иных разрушительных компьютерных кодов, то сразу после их

обнаружения сотрудник обязан:

-проинформировать администратора ЛВС;

- не пользоваться и не выключать зараженный компьютер;

-не подсоединять этот компьютер к компьютерной сети школы до тех пор,

пока на нем не будет произведено удаление обнаруженного вируса и полное

антивирусное сканирование администратором ЛВС.

6.36.

Конфиденциальные встречи (заседания) должны проходить

только в защищенных техническими средствами информационной

безопасности помещениях.

6.37.

Перечень помещений с техническими средствами

информационной безопасности утверждается начальником школы.

6.38.

Участникам заседаний запрещается входить в помещения с

записывающей аудио/видео аппаратурой, фотоаппаратами,

радиотелефонами и мобильными телефонами без предварительного

согласования с администратором ЛВС.

6.39.

Аудио/видео запись, фотографирование во время

конфиденциальных заседаний может вести только сотрудник школы

который отвечает за подготовку заседания, после получения

письменного разрешения руководителя группы организации встречи.

6.40.

Доступ участников конфиденциального заседания в помещение

для его проведения осуществляется на основании утвержденного

перечня, контроль за которым ведет лицо, отвечающее за организацию

встречи.

6.41.

Сотрудникам школы запрещается:

- нарушать информационную безопасность и работу сети школы;

- сканировать порты или систему безопасности;

- контролировать работу сети с перехватом данных;

- получать доступ к компьютеру, сети или учетной записи в обход системы

идентификации пользователя или безопасности;

- использовать любые программы, скрипты, команды или передавать

сообщения с целью вмешаться в работу или отключить пользователя

оконечного устройства;

- передавать информацию о сотрудниках или списки сотрудников школы

посторонним лицам;

- создавать, обновлять или распространять компьютерные вирусы и прочие

разрушительное программное обеспечение.