|  |  |  |  |
| --- | --- | --- | --- |
|  | **УТВЕРЖДАЮ**  %DOLZHNOSTUTVERZH%  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ %FIO%  «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ %year% г. |  |  |

**HE::**

**%SYSTEMORPODSISTEM% ЗАЩИТЫ ИНФОРМАЦИИ**

**%FULLNAMEINFORMATIONSYSTEM%**

**РУКОВОДСТВО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

**%NUMBER\_OF\_CHTZ%.И3**

**Листов 5**

**ОГЛАВЛЕНИЕ**

[1. ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc25782640)

[2. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ 3](#_Toc25782641)

[3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ 4](#_Toc25782642)

[4. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ 4](#_Toc25782643)

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

Руководство администратора безопасности %SHORT\_NAME\_INFSYSTEM% (далее – Руководство) определяет функции, права, обязанности и ответственность администратора безопасности.

Руководство является неотъемлемой частью организационно-распорядительной документации %SHORT\_NAME\_ORGANIZATION%, направленной на обеспечение безопасности информации в %SHORT\_NAME\_INFSYSTEM%.

Администратор безопасности обеспечивает правильное использование и нормальное функционирование установленных средств защиты и контроля защищенности информации, а также осуществляет контроль выполнения требований и организационных мероприятий по обеспечению безопасности информации в %SHORT\_NAME\_INFSYSTEM%.

1. **ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

Администратор безопасности обязан:

* знать состав технических средств, установленных и смонтированных в %SHORT\_NAME\_INFSYSTEM%, перечень используемого программного обеспечения, в том числе средств защиты информации;
* обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
* проводить инструктаж администраторов %SHORT\_NAME\_INFSYSTEM% и обслуживающего персонала по правилам работы в %SHORT\_NAME\_INFSYSTEM% с установленной системой защиты информации (далее – СЗИ);
* инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности или несанкционированного доступа к ресурсам %SHORT\_NAME\_INFSYSTEM%.;
* вести документацию на СЗИ %SHORT\_NAME\_INFSYSTEM% в соответствии с требованиями нормативных документов;
* участвовать в согласовании доступа к защищаемой (конфиденциальной) информации в %SHORT\_NAME\_INFSYSTEM% согласно их правам доступа при получении оформленного соответствующим образом разрешения;
* участвовать в согласовании внесения изменений в конфигурацию%SHORT\_NAME\_INFSYSTEM%;
* анализировать состояние защиты %SHORT\_NAME\_INFSYSTEM% и ее отдельных подсистем;
* осуществлять контроль за подключением информационных систем региональной инфраструктуры электронного правительства в %SHORT\_NAME\_INFSYSTEM% к сетям общего пользования;
* принимать меры по ликвидации последствий в случае возникновения нештатных и аварийных ситуаций;
* проводить расследование при зафиксированных инцидентах информационной безопасности.

Администратор безопасности осуществляет установку, настройку и сопровождение в процессе эксплуатации средства защиты информации в %SHORT\_NAME\_INFSYSTEM%.

В случае отказа средств и систем защиты информации принимает меры по их восстановлению.

Администратор безопасности осуществляет периодическое обновление антивирусных средств, установленных в системе, контроль за соблюдением порядка и правил проведения антивирусных проверок, а также поддержание установленного порядка и правил антивирусной защиты информации в соответствии с внутренними документами по антивирусному контролю в системе.

Администратор безопасности обеспечивает ведение журнала учета машинных носителей информации.

1. **ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

Администратор безопасности имеет право:

* участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
* требовать от администраторов %SHORT\_NAME\_INFSYSTEM% и обслуживающего персонала %SHORT\_NAME\_INFSYSTEM% соблюдения правил обеспечения безопасности информации и выполнения положений организационно-распорядительной документации, направленных на обеспечение безопасности информации в %SHORT\_NAME\_INFSYSTEM%;
* требовать прекращения обработки информации в случае нарушения установленных правил, порядка работ или нарушения функционирования средств и систем защиты информации;
* запрашивать и получать необходимые материалы и документы, относящиеся к вопросам деятельности администратора ИБ;
* взаимодействовать со сторонними учреждениями и организациями для решения оперативных вопросов, входящих в компетенцию администратора безопасности;
* отключать, при участии администраторов %SHORT\_NAME\_INFSYSTEM%, любые элементы средств защиты информации при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей.

При необходимости, администратор безопасности при участии администраторов %SHORT\_NAME\_INFSYSTEM%, имеет право изменять конфигурацию операционных систем, технических и программных средств %SHORT\_NAME\_INFSYSTEM%.

1. **ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

Администратор безопасности несет ответственность за:

* нарушение корректности функционирования средств защиты информации, в соответствии с технической и эксплуатационной документацией;
* несвоевременный анализ произошедших инцидентов и ликвидацию последствий возникновения инцидентов;
* ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных Руководством в соответствии с действующим трудовым законодательством РФ;
* разглашение конфиденциальной информации, ставшей известной ему по роду работы, в соответствии с действующим законодательством РФ.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Лист регистрации изменений*** | | | | | | | | | |
| *Изм.* | *Номера листов (страниц)* | | | | *Всего листов (страниц) в документе* | *Номер документа* | *Входящий номер сопроводительного документа и дата* | *Подпись* | *Дата* |
| *измененных* | *замененных* | *новых* | *аннулированных* |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |