|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**Руководитель службы строительного надзора и жилищного контроля Красноярского края  |
|  | \_\_\_\_\_\_\_\_\_\_\_/ А. Е. Пряничников\_\_\_.\_\_\_.201\_М.П. |

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Службы строительного надзора и жилищного контроля
Красноярского края

(*рабочие материалы*)

2014

ЛИСТ СОГЛАСОВАНИЯ

|  |
| --- |
| **РАЗРАБОТАНО** |
| **Организация-исполнитель** | **Должность исполнителя** | **Фамилия имя, отчество** | **Подпись** | **Дата** |
| ЗАО«РТК-Сибирь» | Начальник отдела защиты информации | ШрамЕвгений Геннадьевич | \_\_\_\_\_\_\_\_\_\_ | \_\_\_.\_\_\_.201\_\_г |
| Заместитель начальника отдела защиты информации | ЛемкеЕвгений Альбертович | \_\_\_\_\_\_\_\_\_\_ | \_\_\_.\_\_\_.201\_\_г |
| Специалист по защите информации 2 категории | КазенниковАлексей Владимирович | \_\_\_\_\_\_\_\_\_\_ | \_\_\_.\_\_\_.201\_\_г |

|  |
| --- |
| **СОГЛАСОВАНО** |
| **Организация-заказчик** | **Должность исполнителя** | **Фамилия имя, отчество** | **Подпись** | **Дата** |
| Служба строительного надзора и жилищного контроля Красноярского края | Начальник отдела анализа и контроля | ПогребнякДенис Константинович | \_\_\_\_\_\_\_\_\_\_ | \_\_\_.\_\_\_.201\_\_г |
| Системный администратор отдела анализа и контроля | Овчинников Владимир Владимирович | \_\_\_\_\_\_\_\_\_\_ | \_\_\_.\_\_\_.201\_\_г |

ОГЛАВЛЕНИЕ

[1 аннотация 4](#_Toc378182637)

[2 список сокращений и обозначений 5](#_Toc378182638)

[3 термины и определения 6](#_Toc378182639)

[4 общие положения 7](#_Toc378182640)

[5 описание объектов защиты 9](#_Toc378182641)

[6 цели и задачи деятельности по обеспечению информационной безопасности 10](#_Toc378182642)

[7 угрозы информационной безопасности 11](#_Toc378182643)

[8 модель нарушителя информационной безопасности 12](#_Toc378182644)

[9 основные положения по обеспечению информационной безопасности 13](#_Toc378182645)

[10 организационная основа деятельности по обеспечению информационной безопасности 16](#_Toc378182646)

[11 ответственность за соблюдение положений политики 19](#_Toc378182647)

[12 контроль за соблюдением положений политики 20](#_Toc378182648)

[13 заключительные положения 21](#_Toc378182649)

# Аннотация

Настоящая Политика информационной безопасности Службы строительного надзора и жилищного контроля Красноярского края (далее – Политика) разработана ЗАО «РТК-Сибирь» в рамках выполнения работ по государственному контракту № 2013.170895 от 07.10.2013 (далее – Контракт) по созданию системы защиты информационных систем Службы строительного надзора и жилищного контроля Красноярского края (далее – Служба) в соответствии с Техническим заданием (Приложение № 1 к Контракту).

# Список сокращений и обозначений

В настоящей Политике используются следующие сокращения:

|  |  |  |
| --- | --- | --- |
| ИБ | - | Информационная безопасность; |
| ЗИ | - | Защита информации; |
| ИС | - | Информационная система; |

# Термины и определения

**Вирус (компьютерный, программный) –** исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Защищаемая информация** –информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информация** – сведения (сообщения, данные) независимо от формы их представления.

**Инцидент информационной безопасности** – появление одного или нескольких событий ИБ, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных ресурсов или инфраструктуры и создания угрозы информационной безопасности.

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Криптосредство** – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

**Модель угроз** – описательное представление свойств или характеристик угроз безопасности информации.

**Модель нарушителя** – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

**Ответственный** – сотрудник Службы, курирующий вопросы информационной безопасности Службы.

**Персональные данные –** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)**.**

**Угроза информационной безопасности** – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу

**Уязвимость** – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

# Общие положения

Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, уполномоченного органа по защите прав субъектов персональных данных и основывается в том числе на:

* Федеральном законе № 149-ФЗ от 27.07.2006г. «Об информации, информационных технологиях и о защите информации»;
* Федеральном законе № 152-ФЗ от 27.07.2006г. «О персональных данных»;
* «Требованиях к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства Российской Федерации № 1119 от 01.11.2012г.);
* «Составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Приказом ФСТЭК России от 18.02.2013г. № 21);
* «Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утв. Приказом ФСТЭК России от 11.02.2013г. № 17);
* «Типовых требованиях по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. руководством 8 Центра ФСБ России 21.02.2008г. № 149/6/6-622);

Настоящая Политика является документом, доступным любому сотруднику Службы и представляет собой официально принятую руководством Службы систему взглядов на обеспечение информационной безопасности, и устанавливает принципы построения системы информационной безопасности на основе систематизированного изложения целей, задач и функций информационной безопасности Службы.

Руководство Службы осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в связи с:

* развитием законодательства и норм регулирования деятельности по защите информации, в том числе по защите персональных данных,
* развитием применяемых в Службе информационных технологий, программных, технических и программно-технических средств обработки информации,

Соблюдение требований информационной безопасности позволит обеспечить функциональную стабильность Службы, соответствие правовым, регулятивным и договорным требованиям. Соблюдение требований информационной безопасности также позволит обеспечить повышение имиджа Службы.

Требования информационной безопасности, которые предъявляются Службой, соответствуют интересам (целям) деятельности Службы и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Службы имеют отношение к:

* организации и реализации процессов обработки информации (в том числе защищаемой),
* взаимоотношениям с юридическими и физическими лицами,
* внутрихозяйственной деятельности Службы.

Факторы рисков в информационной сфере Службы имеют отношение и к иным рискам основной и управленческой деятельности Службы.

Требования Политики информационной безопасности Службы должны неукоснительно соблюдаться всеми сотрудниками Службы и другими сторонами как это определяется положениями внутренних нормативных документов Службы, а также требованиями договоров и соглашений, стороной которых Служба является.

Настоящая Политика распространяется на процессы обработки информации в Службе и обязательна для применения всеми сотрудниками и руководством Службы, а также пользователями ее информационных ресурсов.

Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в филиалах и представительствах Службы.

Настоящая Политика является основополагающим документом по ИБ в Службе.

Документы, детализирующие положения Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Службы, должны основываться на положениях настоящей Политики, оформляться как отдельные внутренние нормативные документы Службы, разрабатываться, согласовываться и утверждаться в соответствии с установленным в Службе порядком.

# Описание объектов защиты

Основными объектами защиты системы информационной безопасности в Службе являются:

* информационные ресурсы, содержащие персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Службы, независимо от формы и вида ее представления;
* сотрудники Службы, являющиеся разработчиками и пользователями информационных систем Службы;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

# Цели и задачи деятельности по обеспечениюинформационной безопасности

Целью деятельности по обеспечению информационной безопасности Службы является снижение угроз информационной безопасности до приемлемого для Службы уровня.

Основные задачи деятельности по обеспечению информационной безопасности Службы:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение угроз информационной безопасности либо минимизация вероятности их возникновения.

# Угрозы информационной безопасности

Все множество потенциальных угроз ИБ делится на три класса по природе их возникновения: антропогенные, техногенные и природные.

7.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.д., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, которые могут быть связаны с:

* нестабильностью и противоречивостью требований регуляторов деятельности Службы и контрольных органов,
* с несогласованностью действий в руководстве и управлении Службой,
* неадекватными целям по отношению к той или иной сложившейся ситуации
* с потребляемыми услугами, с человеческим фактором.

7.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

7.3 Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре Службы могут быть как внешними, так и внутренними.

При разработке систем (подсистем) защиты информации, должны составляться документы, определяющие угрозы безопасности, характерные для конкретного вида защищаемой информации, при ее обработке в информационных системах Службы.

# Модель нарушителя информационной безопасности

По отношению к Службе нарушители ИБ могут быть разделены на внешних и внутренних нарушителей.

8.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Службой рассматриваются:

* зарегистрированные пользователи информационных систем Службы;
* сотрудники Службы, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Службы, но имеющие доступ в здания и помещения Службы;
* персонал, обслуживающий технические средства информационных систем Службы;
* сотрудники самостоятельных структурных подразделений Службы, задействованные в разработке и сопровождении программного и/или аппаратного обеспечения;
* руководители различных уровней.

8.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей Службой рассматриваются:

* бывшие сотрудники Службы;
* представители организаций, взаимодействующих по вопросам технического обеспечения Службы;
* лица, обратившиеся в Службу по вопросам, связанным с ее целевой деятельностью;
* посетители зданий и помещений Службы;
* члены преступных организаций, сотрудники иностранных спецслужб или лица, действующие по их поручению;
* лица, случайно или умышленно проникшие в информационную систему Службы из внешних телекоммуникационных сетей («хакеры»).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

* нарушитель скрывает свои несанкционированные действия от других сотрудников Службы;
* несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
* в своей деятельности вероятный нарушитель может использовать любое имеющееся в свободной продаже средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
* внешний нарушитель может действовать в сговоре с внутренним нарушителем.

При разработке систем (подсистем) защиты информации, должны составляться документы, определяющие модель нарушителя безопасности, характерную для конкретного вида защищаемой информации, при ее обработке в информационных системах Службы.

# Основные положения по обеспечению информационной безопасности

9.1. Требования об обеспечении информационной безопасности Службы обязательны к соблюдению всеми сотрудниками Службы и пользователями информационных систем Службы.

Руководство Службы приветствует и поощряет в установленном порядке деятельность сотрудников Службы и пользователей информационных систем по обеспечению информационной безопасности.

Неисполнение или некачественное исполнение сотрудниками Службы и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Службе порядком, либо требованиями действующего законодательства.

Стратегия Службы в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению информационной безопасности: от организационных мер на уровне руководства Службы, до специализированных программных и/или технических мер информационной безопасности по каждой выявленной в Службе угрозе информационной безопасности.

С целью поддержки заданного уровня защищенности, Служба придерживается функционального подхода в построении системы информационной безопасности.

Система информационной безопасности Службы основывается на осуществлении следующих основных функций:

* планирование мер по информационной безопасности,
* реализация мер по информационной безопасности,
* проверка выполнения мер по информационной безопасности,
* совершенствование мер по информационной безопасности,

соответствующих требованиям законодательства Российской Федерации по информационной безопасности.

На всех этапах жизненного цикла системы информационной безопасности Службы соблюдаются требования настоящей Политики.

9.2. При планировании мероприятий по обеспечению информационной безопасности в Службе осуществляются:

9.2.1. Определение и распределение ролей сотрудников Службы, связанных с обеспечением информационной безопасности.

9.2.2. Оценка важности информационных ресурсов с учетом потребности в обеспечении их свойств (конфиденциальности, целостности, доступности) с точки зрения информационной безопасности.

9.2.3. Управление информационной безопасностью, включающее:

* анализ влияния на информационную безопасность Службы применяемых в деятельности Службы технологий, а также внешних по отношению к Службе событий;
* выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
* определение моделей угроз информационной безопасности Службы;
* выявление, анализ и оценка значимых для Службы угроз информационной безопасности;
* выявление возможных негативных последствий для Службы, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных ресурсов Службы;
* идентификацию и анализ событий информационной безопасности;
* оценку угроз информационной безопасности и определение среди них неприемлемых для Службы;
* оценку влияния мер по ЗИ на цели основной деятельности Службы;
* оценку затрат на реализацию мер по ЗИ;
* рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
* разработку планов управления различными защитными мерами и вариантами их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Службы и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
* документальное оформление целей и задач обеспечения информационной безопасности Службы, поддержка в актуальном состоянии нормативно-методического обеспечения деятельности в сфере информационной безопасности.

9.3. В рамках реализации деятельности по обеспечению информационной безопасности в Службе осуществляются:

9.3.1. Управление инцидентами информационной безопасности, включающее:

* сбор информации о событиях информационной безопасности;
* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инциденты информационной безопасности;
* минимизация негативных последствий инцидентов информационной безопасности;
* оперативное доведение до руководства Службы информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
* выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
* пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

9.3.2. Повышение уровня знаний сотрудников Службы по вопросам обеспечения информационной безопасности;

9.3.3. Обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Службы и информации, обрабатываемой в них;

9.3.4. Применение программных, аппаратных и программно-аппаратных (в том числе криптографических) средств защиты информации;

9.3.5. Обеспечение бесперебойной работы информационных систем и сетей связи в том числе включающее:

* обеспечение резервирования защищаемой информации;
* обеспечение возобновления работы информационных систем и сетей связи после прерываний и нештатных ситуаций;

9.3.6. Применение средств защиты информации от вредоносных программ;

9.3.7. Обеспечение информационной безопасности на всех стадиях жизненного цикла информационных систем Службы, связанных с их проектированием, разработкой, приобретением, поставкой, вводом в действие и сопровождением (сервисным обслуживанием);

9.3.8. Обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

9.3.9. Контроль доступа в здания и помещения Службы.

9.4. В рамках проведения проверки выполнения мер по информационной безопасности в Службе осуществляются:

* контроль правильности реализации и эксплуатации мер по защите информации;
* контроль изменений конфигурации систем и подсистем Службы;
* контроль реализации и исполнения требований сотрудниками Службы действующих внутренних нормативных документов по обеспечению информационной безопасности;
* контроль деятельности сотрудников и других пользователей информационных систем Службы, направленный на выявление и предотвращение инцидентов ИБ.

9.5. В целях совершенствования деятельности по обеспечению информационной безопасности в Службе осуществляется:

* периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Службы);
* периодическое, а при необходимости оперативное, уточнение/пересмотр угроз информационной безопасности (при изменениях целей и задач основной деятельности Службы);
* периодическое повышение уровня квалификации сотрудников Службы, отвечающих за информационную безопасность, в том числе с прохождением специализированных курсов;

# Организационная основа деятельности по обеспечению информационной безопасности

10.1. В целях выполнения задач по обеспечению информационной безопасности Службы, в соответствии с требованиями законодательства РФ по информационной безопасности, а также рекомендациями стандартов по информационной безопасности в Службе определяются следующие роли:

* **Ответственный** за обеспечение информационной безопасности Службы (далее – Ответственный);
* **Администратор информационной безопасности** Службы (далее – Администратор ИБ);
* **Администратор информационных систем** Службы (далее – Администратор ИС);
* **Пользователь** информационных систем Службы (далее – пользователь).

При необходимости могут быть определены и другие роли по информационной безопасности.

10.2. Задачами Ответственного являются:

* назначение ответственных лиц в области ИБ;
* координация внедрения систем информационной безопасности в Службе;
* курирование вопросов по информационной безопасности в Службе;
* установление потребностей Службы в применении мер по обеспечению информационной безопасности, определяемых как внутренними требованиями, так и требованиями нормативных актов законодательства РФ;
* соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации;
* разработка (согласование) и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Службы, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов по вопросам информационной безопасности;
* осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Службы;

10.3. Задачами администратора ИБ являются:

* планирование эксплуатации и участие в поставке средств обеспечения информационной безопасности на объектах и системах Службы;
* обучение, контроль и непосредственная работа с сотрудниками Службы по вопросам информационной безопасности;
* выявление и предотвращение угроз информационной безопасности;
* выявление и реагирование на инциденты информационной безопасности;
* информирование в установленном порядке Ответственного об угрозах информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности;
* пресечение несанкционированных действий нарушителей информационной безопасности;
* поддержка в актуальном состоянии базы инцидентов информационной безопасности (в бумажном или электронном виде), анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
* типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на отделы Службы;
* обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
* мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности мер по ЗИ;
* периодический анализ электронных журналов средств защиты информации, применяемых в Службе, на предмет несанкционированного доступа;
* контроль обеспечения информационной безопасности Службы, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
* информирование руководства Службы и руководителей его самостоятельных структурных подразделений об угрозах информационной безопасности, влияющих на деятельность Службы.

10.4. Основными задачами Администратора ИС Службы при выполнении возложенных на него обязанностей и в рамках его участия в оперативной деятельности по обеспечению информационной безопасности Службы являются:

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Службы;
* заведение в информационных системах Службы учетных записей пользователей и их удаление из информационных систем Службы;
* осуществление резервного копирования защищаемой информации в информационных системах Службы по согласованию с Администратором ИБ и/или Ответственным;
* установка и настройка программных продуктов (за исключением средств защиты информации), используемых Службой в рамках своей деятельности;
* разработка и согласование планов по изменению программной и/или аппаратной конфигурации ИС Службы (с отражением анализа потенциального воздействия таких изменений);
* мониторинг и оценка состояния технических и программных средств информационных систем Службы;
* обучение и непосредственная работа с пользователями ИС Службы по вопросам функционирования и эксплуатации программных продуктов и технических средств;

10.5. Основными задачами пользователей информационных систем Службы при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности Службы являются:

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Службы;
* выявление и предотвращение угроз информационной безопасности в пределах своей компетенции;
* выявление и реагирование на инциденты информационной безопасности в пределах своей компетенции;
* информирование в установленном порядке ответственных лиц (Ответственного или Администратора ИБ) о выявленных угрозах информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
* мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;

10.6. Планирование деятельности по обеспечению информационной безопасности Службы осуществляется и координируется Ответственным.

10.7. Ответственный может создавать оперативные группы для проведения расследований инцидентов информационной безопасности и, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, может привлекать для работы в таких группах любых сотрудников Службы на основе совмещения работы в группе со своими основными должностными обязанностями. Такие оперативные группы могут возглавляться как Ответственным, так и иными лицами по согласованию с Ответственным или руководителем Службы.

10.8. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках основного бюджета Службы.

# Ответственность за соблюдение положений Политики

Общее руководство обеспечением информационной безопасности Службы осуществляет Ответственный.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в управление информационной безопасности Службы лежит на руководстве Службы.

Ответственность сотрудников Службы за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры (контракты) с сотрудниками Службы, а также положениями внутренних нормативных документов Службы.

# Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности Службы осуществляется Ответственным.

Текущий контроль соблюдения настоящей Политики осуществляется Ответственным и Администратором ИБ Службы, а также Администратором ИС и пользователями ИС в пределах их компетенции.

Ответственный и Администратор ИБ осуществляют контроль соблюдения настоящей Политики на основе проведения периодического мониторинга и внутреннего аудита состояния информационной безопасности Службы.

# Заключительные положения

Требования настоящей Политики могут развиваться другим внутренними нормативными документами Службы, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также Положения о Службы настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Положению о Службе. В этом случае Ответственный обязан незамедлительно инициировать внесение соответствующих изменений.

Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

* периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
* внеплановое внесение изменений в настоящую Политику может осуществляться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Ответственность за внесение изменений в настоящую Политику возлагается на Ответственного за обеспечение информационной безопасности Службы.