Выписка из Политики информационной безопасности ФАУ «Главгосэкспертиза России», утвержденной приказом от 26.02.2018 № 41

Политика информационной безопасности регулирует организацию деятельности ФАУ «Главгосэкспертиза России» (далее – Учреждение) в области обеспечения информационной безопасности и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

Положения Политики информационной безопасности распространяются на все области деятельности, всех работников, используемые информационные системы, средства коммуникации и помещения Учреждения, за исключением связанных с защитой сведений, составляющих государственную тайну.

Целью обеспечения информационной безопасности в Учреждении является защита Учреждения в процессе осуществления им уставной деятельности от возможного нанесения ему значимого ущерба в результате случайной или преднамеренной реализации угроз в информационной сфере, направленных на несанкционированное вмешательство в процессы обработки информации и процессы функционирования компонентов ИТ-инфраструктуры.

Указанная цель достигается путем выполнения следующих задач:

- обеспечение выполнения требований государственного регулирования в области защиты информации в соответствии с законами Российской Федерации, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, нормативными документами Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации;
- фиксация в разрабатываемых внутренних нормативных документах всех требований информационной безопасности;
- управление рисками информационной безопасности Учреждения;
- выбор мер обеспечения информационной безопасности с учетом снижения вероятности возникновения угроз информационной безопасности и возможных последствий от их реализации;
- реагирование на инциденты информационной безопасности с целью предотвращения и/или снижения ущерба от них;
- проведение внутренних и внешних аудитов информационной безопасности Учреждения;
- постоянное и непрерывное совершенствование комплексной системы управления информационной безопасности Учреждения;
- повышение осведомленности в вопросах информационной безопасности работников структурных подразделений Учреждения.

В основе подхода к управлению и обеспечению информационной безопасности лежит необходимость определить, реализовать, эксплуатировать и совершенствовать организационно-технический комплекс защитных мер в отношении информации, обрабатываемой в Учреждении.

В основе комплексной системы управления информационной безопасности Учреждения лежит модель, затрагивающая все вопросы управления информационной безопасности:

- выделение и официальное назначение представителей структурных подразделений Учреждения, отвечающих за вопросы внедрения, эксплуатации и контроля обеспечения информационной безопасности;
- регламентирование действий по вопросам контроля и оценки процессов разработки, внедрения, функционирования, мониторинга, анализа, поддержки и совершенствования информационной безопасности;
- доведение регламентированных требований до всех работников Учреждения и периодический контроль знаний;
- выполнение регламентированных требований и контроль их выполнения.

Организационная составляющая комплекса мер в области защиты информации в Учреждении опирается на четко выстроенный циклический процесс управления информационной безопасности, основанный на модели Деминга–Шухарта.

Система обеспечения информационной безопасности включает в себя:

- технические средства информационной безопасности (аппаратно-программные, инженерно-технические);
- документы технического характера по информационной безопасности, в том числе регламентирующие порядок внедрения и использования (сопровождения) средств и мер информационной безопасности;
- персонал, администрирующий технические средства информационной безопасности.

Необходимый состав функций по технической защите информации, которые реализованы в системе обеспечения информационной безопасности, определяется в соответствии с требованиями законодательства и нормативно-правовых актов, регулирующих вопросы защиты информации, а также на основе анализа актуальных угроз и оценки рисков информационной безопасности.