Головинский Анатолий Александрович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Синяков Евгений Анатольевич
Преподаватель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Чухров Роман Вячеславович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Кузнецов Илья Олегович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ В ИНТЕРЕСАХ ОРГАНА БЕЗОПАСНОСТИ ПРИ СОЗДАНИИ В ЕГО СТРУКТУРЕ ПОДРАЗДЕЛЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: создание подразделения криптографической защиты информации (КЗИ) в структуре органа безопасности представляет собой комплексный процесс, включающий нормативно-правовую, организационно-штатную, техническую и кадровую подготовку.

Ключевые слова: криптографическая защита, орган безопасности, подразделение, информационная безопасность, внедрение, мероприятия.

Создание подразделения криптографической защиты информации (КЗИ) в структуре органа безопасности является ответом на растущие требования к обеспечению конфиденциальности, целостности и доступности информации, циркулирующей в ведомственной и государственной инфраструктуре. Это мероприятие требует системного и поэтапного подхода, охватывающего нормативную, кадровую, техническую и организационную составляющие.

Криптографическая защита требует высокого уровня профессионализма. Поэтому особое внимание уделяется подбору и подготовке кадров:

Подразделение КЗИ должно развиваться синхронно с изменяющейся ИТ-инфраструктурой и угрозами информационной безопасности.

В первую очередь осуществляется анализ действующего законодательства и нормативных правовых актов, регулирующих использование средств криптографической защиты. Важным этапом становится подготовка внутренней нормативной базы, включая разработку положения о новом подразделении, определение его задач, функций и порядка взаимодействия с другими элементами органа безопасности. Также требуется согласование документации с профильными ведомствами, такими как ФСТЭК России и ФСБ России, особенно в части использования сертифицированных средств криптографической защиты (СКЗИ) и получения лицензий, если деятельность подразделения предполагает выполнение работ, подлежащих обязательному лицензированию.

Параллельно формируется организационно-штатная структура нового подразделения. Определяются должности, квалификационные требования к сотрудникам, зоны ответственности и функциональное распределение ролей. Особое внимание уделяется подбору кадров – специалисты по криптографической защите должны не только обладать профильным образованием и опытом работы, но и иметь допуск к сведениям, составляющим государственную тайну. Подразделение должно включать как технических специалистов, так и руководителей, способных координировать взаимодействие с другими звеньями системы безопасности.

Техническое оснащение подразделения включает в себя приобретение, внедрение и настройку сертифицированных СКЗИ, а также создание защищённых каналов связи и хранилищ ключевой информации. Рабочие места сотрудников подразделения должны быть оборудованы в соответствии с требованиями нормативных документов по защите информации, в том числе с учётом требований по физической защите и контролю доступа. Дополнительно организуются меры по защите от несанкционированного доступа, внешнего вмешательства и технических утечек информации.

После создания подразделения проводится его интеграция в общую систему информационной безопасности органа. Подразделение КЗИ должно быть включено в модель угроз, участвовать в планировании мероприятий по обеспечению безопасности, а также в реагировании на инциденты. Разрабатываются процедуры внутреннего контроля, ведется мониторинг эффективности применения криптографических средств, а также реализуются мероприятия по регулярной аттестации и проверке технических решений на соответствие установленным требованиям.

Важной частью деятельности подразделения является обучение и повышение квалификации сотрудников. Организуются курсы, семинары и инструктажи, как для специалистов подразделения, так и для других сотрудников органа безопасности, использующих СКЗИ в своей деятельности. Это обеспечивает единообразное понимание целей и методов криптографической защиты, а также снижает риски ошибок, связанных с человеческим фактором.

Таким образом, создание подразделения КЗИ в структуре органа безопасности требует реализации целого комплекса мероприятий. Успешность этого процесса зависит от координации между структурами, точного соблюдения нормативных требований, обеспечения материально-технической базы и грамотного управления персоналом. Правильно организованное подразделение криптографической защиты становится важным элементом системы национальной и ведомственной безопасности, существенно повышающим устойчивость к современным информационным угрозам.

Список литературы:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2022681284 Российская Федерация. Программа по учету средств криптографической защиты информации: № 2022680691: заявл. 24.10.2022: опубл. 11.11.2022 / А. В. Акишин, Н. Н. Енин, С. Н. Ершов [и др.]. – EDN QIXXPV.

2. Свидетельство о государственной регистрации базы данных № 2019621548 Российская Федерация. Информационная система по учету и обработке данных для подразделений защиты информации ("Akishin_LS 8.0"): № 2019621403: заявл. 15.08.2019: опубл. 02.09.2019 / А. А. Бречко, Р. Д. Фатьянов, И. А. Федяева [и др.]. – EDN YTQUXF.

3. Свидетельство о государственной регистрации программы для ЭВМ № 2024618327 Российская Федерация. Информационно-справочная система учета движения МНИ в организациях: № 2024617042: заявл. 01.04.2024: опубл. 10.04.2024 / Е. В. Якель, Д. П. Нечаев, М. С. Бодякин [и др.]; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации. – EDN SOGRCQ.

4. Анализ проблем применения программного обеспечениядля создания систем поддержки принятия решений должностных лиц подразделений информационной безопасности / Д. А. Охотин, А. В. Акишин, Е. С. Уколов [и др.] // Вектор научной мысли. – 2025. – № 1 (18). – С. 323-325. – EDN EFSNBN.

5. Свидетельство о государственной регистрации программы для ЭВМ № 2023669474 Российская Федерация. Программа поддержки принятия решений руководителя подразделения информационной безопасности: № 2023668535: заявл. 30.08.2023: опубл. 14.09.2023 / А. В. Акишин, Д. А. Ржевский, Р. В. Лукьянов [и др.]. – EDN DHOEBO.