Сбитнев Егор Алексеевич,
Преподаватель, КВВУ им. Штеменко

Акишин Андрей Владимирович,
Доцент, КВВУ им. Штеменко

Дубовцов Иван Андреевич,
Преподаватель, КВВУ им. Штеменко

Лукьянов Роман Васильевич,
Преподаватель, КВВУ им. Штеменко

Пискарев Владислав Сергеевич,
Слушатель, КВВУ им. Штеменко

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ РУКОВОДИТЕЛЮ ПОДРАЗДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ПО ОРГАНИЗАЦИИ И КОНТРОЛЮ СОБЛЮДЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ ОБРАЩЕНИИ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье представлен системный подход к организации повседневной деятельности руководителя подразделения информационной безопасности в части контроля конфиденциальности при эксплуатации СКЗИ. На основе актуальных нормативных актов ФСБ даны конкретные алгоритмы назначения ответственных, ведения учета, проведения проверок и реагирования на инциденты.

Ключевые слова: Конфиденциальность информации, средства криптографической защиты информации (СКЗИ), обращение с СКЗИ, учет ключевой документации, инциденты информационной безопасности.

Современное состояние защищенности информации на предприятиях, обрабатывающих конфиденциальные данные, требует от руководителя подразделения информационной безопасности (ИБ) не только технической компетенции, но и умения выстроить жесткую организационно-распорядительную систему. Наиболее уязвимым звеном в этой системе является повседневное обращение сотрудников со средствами криптографической защиты информации (СКЗИ). Ошибки в хранении ключей, нерегулярный учет, отсутствие контроля за действиями пользователей приводят к компрометации шифров и, как следствие, к утечке информации.

Цель данных рекомендаций – предоставить практический инструментарий для организации и контроля конфиденциальности информации при обращении с СКЗИ в повседневной деятельности, исключающий формальный подход.

Ключевой элемент контроля конфиденциальности – персональная ответственность. Руководитель подразделения ИБ обязан издать приказ по предприятию (или распоряжение), в котором назначить:

1. Лицо, ответственное за обращение с СКЗИ (далее – Ответственный). Это, как правило, сотрудник подразделения ИБ. Его функции: учет, хранение, выдача и прием СКЗИ, ведение журналов, контроль целостности упаковки ключевых носителей.
2. Администратора СКЗИ (может совмещать функции с Ответственным, но при большом парке – отдельно). Задачи: инсталляция, настройка, обновление криптомодулей, обеспечение совместимости с аттестованным ПО.

3. Пользователей СКЗИ – конкретный перечень сотрудников, допущенных к работе с криптосредствами. Каждый пользователь должен быть ознакомлен под подпись с инструкцией.

Бесконтрольное обращение с криптосредствами – главная угроза конфиденциальности. Приказ № 117 (2025) вводит обязательную маркировку каждого экземпляра СКЗИ уникальным номером. Руководитель подразделения ИБ должен организовать следующие процедуры.

1. Внедрите два отдельных журнала:

1.1 Журнал учета СКЗИ (в бумажном виде, страницы пронумерованы, прошнурованы, скреплены печатью). Записи: дата поступления, наименование, заводской номер, уникальный учетный номер предприятия, сведения о выданном пользователе, дата возврата, отметка об утилизации.

1.2 Журнал учета ключевых документов (ключей шифрования, паролей, ПИН-кодов, ключевых носителей). Запрещено записывать сами ключи в открытом виде. Фиксируется только факт выдачи носителя (токена, дискеты) с указанием его идентификатора.

2. СКЗИ и ключевая документация должны храниться раздельно. Используйте металлические сейфы (шкафы), опечатываемые Ответственным. В повседневной деятельности:

2.1 Пользователи получают СКЗИ на время выполнения задачи (например, на рабочую смену).

2.2 По окончании работы СКЗИ и все ключевые носители подлежат обязательному возврату Ответственному.

2.3 Запрещается оставлять СКЗИ на рабочем столе, в незапираемых ящиках, передавать коллегам.

3. Проведение инвентаризаций

Руководитель подразделения ИБ назначает ежеквартальные (или ежемесячные при высокой интенсивности) внезапные проверки наличия СКЗИ у пользователей. Результат оформляется актом. При выявлении недостачи – немедленный доклад руководству и уведомление территориального органа ФСБ в течение 24 часов (по приказам № 524 и № 117).

4. утвердить документ «Инструкция пользователя СКЗИ», который в обязательном порядке содержит следующие запреты и предписания (в соответствии с п. 17-20 Приказа № 524 и п. 24-26 Приказа № 117):

Запрещено:

1. записывать ключевую информацию на неучтенные съемные носители;
2. использовать личные (некорпоративные) носители для работы с СКЗИ;
3. сообщать пароли, ключи, ПИН-коды любым третьим лицам, включая руководителя ИБ (исключение – передача ключей в опечатанном виде через Ответственного);
4. оставлять сеанс шифрованной связи без контроля, если не активирован автоматический блокиратор экрана;
5. подключать СКЗИ к неаттестованному оборудованию (например, к домашнему ПК).

Предписано:

1. при уходе с рабочего места (даже на 5 минут) закрыть криптоконтейнер или выгрузить ключи из оперативной памяти;
2. немедленно докладывать Ответственному о любых сбоях в работе СКЗИ;
3. ежедневно в конце рабочего дня сдавать СКЗИ и ключевые носители.

Несмотря на профилактику, инциденты возможны. Типовые ситуации: утеря токена с ключом, сбой в работе СКЗИ, некорректное отображение шифротекста, подозрение на компрометацию.

В соответствии с Приказом № 66 (раздел «Эксплуатация») и новыми требованиями № 117, руководитель подразделения ИБ обязан действовать по жесткому алгоритму:

Шаг 1. Обнаружение и локализация. Пользователь немедленно (в течение 15 минут) докладывает Ответственному или руководителю ИБ. Рабочее место изолируется: отключается от сети, опечатывается (пломбируется). Запрещены любые действия с СКЗИ до прибытия руководителя ИБ.

Шаг 2. Внутреннее расследование. Руководитель подразделения ИБ создает комиссию. Задачи: установить причины, время, круг лиц, имевших доступ, оценить факт компрометации (был ли доступ к ключам у посторонних).

Шаг 3. Уведомление ФСБ. При подтверждении утраты или компрометации – в течение 24 часов направляется письменное уведомление в территориальный орган ФСБ (по форме, согласованной с управлением). К уведомлению прилагаются копии акта расследования.

Шаг 4. Замена ключей. По согласованию с ФСБ (или в соответствии с регламентом) проводится экстренная смена всех компрометированных ключей. Пользователь, допустивший утрату, отстраняется от работы с СКЗИ.

Шаг 5. Меры дисциплинарного воздействия. Руководитель подразделения ИБ готовит представление на имя директора предприятия о применении взыскания (вплоть до увольнения) и о необходимости возмещения материального ущерба (стоимость СКЗИ и затрат на замену ключей).

Руководитель подразделения ИБ обязан организовать регулярное повышение квалификации. Не реже одного раза в полугодие проводятся:

1. инструктажи с пользователями (с акцентом на типичные ошибки);
2. тренировки по действиям при компрометации (учебная тревога);
3. курсы повышения квалификации для самого руководителя и его заместителей по новым приказам ФСБ.

Организация и контроль соблюдения конфиденциальности информации при обращении с СКЗИ в повседневной деятельности – это не разовое мероприятие, а непрерывный управленческий процесс. Руководитель подразделения ИБ выступает в роли главного архитектора этой системы. Он должен обеспечить:

1. четкое распределение ответственности;
2. неукоснительное ведение журналов и инвентаризаций;
3. ежедневный контроль возврата СКЗИ;
4. готовность к инцидентам (уведомление ФСБ за 24 часа);
5. постоянное обучение персонала.

Только такой системный подход гарантирует, что даже в рутинных операциях шифрования информация останется конфиденциальной, а предприятие избежит репутационных и финансовых потерь, а также санкций со стороны регулирующих органов

Список литературы:

1. Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

2. Приказ Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».

3. Приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

4. 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.

5. 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.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2020610526 Российская Федерация. Программное средство синтеза (формирования) состава и структуры системы контроля защищенности: № 2019667254: заявл. 25.12.2019: опубл. 15.01.2020 / А.В. Акишин. – EDN EJUDNK