

Памятка
по эксплуатации средств криптографической защиты информации
ViPNet Client и дистрибутивов ключей к ним.

1. Термины и сокращения, используемые в настоящей памятке:

СКЗИ	Средство криптографической защиты информации, сертифицированное ФСБ России (в рамках данной памятки – ViPNet Client)
Дистрибутив ключей	Носитель с комплектом ключевой информации пользователя, ключей узлов, справочников и лицензии.
Пользователь СКЗИ	Работник, получивший дистрибутив ключей и допущенный к работе с СКЗИ «ViPNet Client»
Спецпомещение	Помещение, в котором используются или хранятся СКЗИ и дистрибутивы ключей.
ОКЗ	Орган криптографической защиты информации, создаваемый в организации, в состав которого обычно входят сотрудники отдела информационной безопасности (также функции ОКЗ могут быть возложены на физическое лицо).

Перечень пользователей СКЗИ и перечень Спецпомещений и допущенных в них сотрудников утверждается приказом руководителя организации.

2. Обязанности ОКЗ

- 2.1. Вести поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним.
- 2.2. Обучать пользователей работе с СКЗИ и проверять готовность пользователей к самостоятельному использованию СКЗИ с составлением соответствующих заключений о возможности эксплуатации СКЗИ.
- 2.3. Выдавать экземпляры СКЗИ, эксплуатационной и технической документации к ним, дистрибутивы ключей пользователям под расписку в соответствующем журнале поэкземплярного учета.
- 2.4. Осуществлять установку, настройку и ввод в эксплуатацию СКЗИ с составлением соответствующих актов.
- 2.5. Осуществлять контроль за соблюдением правил безопасной эксплуатации СКЗИ.

3. Обязанности пользователей СКЗИ

- 3.1. Хранить выданные дистрибутивы ключей, установочные диски СКЗИ и документацию в шкафах индивидуального пользования, оборудованных опечатавающими устройствами.
- 3.2. Вести журнал учета доступа к шкафу индивидуального пользования.
- 3.3. Не допускать компрометации СКЗИ и дистрибутивов ключей. Под компрометацией понимается хищение, утрата, разглашение, несанкционированное копирование и другие действия, в результате которых СКЗИ могут стать доступными посторонним лицам и (или) процессам.
- 3.4. Не допускать копирования информации с дистрибутивов ключей или установочных дисков СКЗИ или записи какой-либо информации на эти носители или установочные диски СКЗИ.
- 3.5. Дистрибутивы ключей использовать только на своем рабочем месте.

3.6. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или дистрибутивах ключей (а также парольной информации к ним) сотрудникам(у) ОКЗ.

3.7. Проверять целостность пломб-наклеек на системных блоках, а при наличии признаков их вскрытия – уведомлять ОКЗ.

3.8. Немедленно уведомлять ОКЗ о фактах утраты установочных дисков СКЗИ или документации к ним, дистрибутивов ключей, ключей от помещений, ключей от шкафов индивидуального пользования, личных печатей-пломбиров и о других фактах, которые могут привести к негативным последствиям для информационной безопасности.

3.9. При увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать установочные диски СКЗИ, документацию к ним, дистрибутивы ключей, ключи от помещений и шкафов индивидуального пользования.

4. Требования к Спецпомещениям

4.1. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Спецпомещений в нерабочее время.

4.2. Окна Спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Спецпомещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Спецпомещения.

4.3. Должна быть исключена возможность неконтролируемого проникновения или пребывания в Спецпомещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.4. Двери Спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

4.5. Для предотвращения просмотра извне Спецпомещений их окна должны быть защищены жалюзи, шторами.

4.6. По окончании рабочего дня двери Спецпомещения и установленные в них шкафы индивидуального пользования должны быть заперты и опечатаны, а в журналы учета доступа внесены записи о закрытии.

5. Ответственность

5.1. Допущенные в Спецпомещения несут персональную ответственность за сохранность ключей от помещений и личных печатей-пломбиров, а также за допущение бесконтрольного нахождения в Спецпомещениях посторонних лиц.

5.2. Пользователи СКЗИ кроме ответственности, предусмотренной п. 5.1 настоящей памятки, также несут персональную ответственность за сохранность установочных дисков СКЗИ, документации к ним, дистрибутивов ключей, ключей от шкафов индивидуального пользования.

5.3. Пользователи СКЗИ несут ответственность за несоблюдение обязанностей, перечисленных в п. 3 настоящей памятки.

5.4. Нарушение требований нормативных правовых документов Российской Федерации в области информационной безопасности предусматривает гражданско-правовую, административную и уголовную ответственность.