ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)

УТВЕРЖДАЮ
Директор ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)
_____ С.И. Василиади
«10» января 2026 г.

ПРОГРАММА ОБУЧЕНИЯ

«Использование средств криптографической защиты информации в защищённом документообороте»

Вид: программа повышения осведомлённости пользователей (не является дополнительной профессиональной программой).

Показатель	Значение
Объём	16 учебных часов
Форма обучения	Заочная, с применением электронного обучения и дистанционных образовательных технологий
Способ реализации	Дистанционно: электронные материалы, консультации, практические задания и дистанционный контроль
Категория слушателей	Работники организаций, использующие средства криптографической защиты информации, электронную подпись и защищённый электронный документооборот.
Порядок допуска	Без образовательного ценза ДПО
Итоговый документ	Документ о прохождении инструктажа/обучения либо справка по локальному порядку (не удостоверение о ПК)

1. Общая характеристика и цель

Цель: Повышение осведомлённости пользователей о безопасном обращении со средствами криптографической защиты, ключевыми носителями и документами в защищённом документообороте.

Продолжительность и учебный график устанавливаются настоящей программой; даты проведения занятий определяются расписанием конкретной группы. Учёт трудоёмкости ведётся в учебных часах. Для занятий применяется академический час 45 минут.

Программа направлена исключительно на повышение осведомлённости и формирование безопасных пользовательских привычек. Освоение не подтверждает новую квалификацию и не заменяет специальную подготовку администраторов средств криптографической защиты.

2. Планируемые результаты

Результаты обучения:

- РО1. Распознавать нарушения правил использования ключевых носителей и электронной подписи.
- РО2. Следовать инструкции по безопасному обмену электронными документами.
- РО3. Своевременно информировать ответственных лиц о подозрительных событиях.

По завершении обучения слушатель должен знать: базовые правила использования СКЗИ и электронной подписи, риски компрометации ключей и порядок сообщения о подозрительных событиях.

По завершении обучения слушатель должен уметь: проверять адресата электронного документа, защищать ключевой носитель, применять корпоративный порядок подтверждения операций и информирования об инцидентах.

3. Учебный план

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
1	Базовые правила защищённого документооборота	3	1	1	1	Текущий контроль
2	Ключи, сертификаты и носители	4	1	2	1	Текущий

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
						контроль
3	Практика защищённого обмена документами	4	1	2	1	Текущий контроль
4	Инциденты и социальная инженерия	3	1	1	1	Текущий контроль
	Итоговая проверка	2	0	2	0	Тест и кейс
	ВСЕГО	16	4	8	4	

Теор. — теоретическое освоение материала; практ. — практические занятия и задания с обратной связью; самост. — самостоятельная работа. Итоговый контроль включён в общую трудоёмкость.

4. Календарный учебный график

Период	Объём, ч.	Модули/контроль (№ и часы)
Неделя 1	16	1 (3 ч.); 2 (4 ч.); 3 (4 ч.); 4 (3 ч.); 5 (2 ч.)

График рассчитан из условной нагрузки не более 30 учебных часов в неделю. При формировании учебной группы конкретные даты и распределение занятий утверждаются расписанием без изменения общей трудоёмкости и итоговых результатов.

5. Рабочие программы дисциплин (модулей)

Модуль 1. Базовые правила защищённого документооборота — 3 ч.

Содержание: Роли пользователя, администратора и подписанта; Типовые угрозы при обмене документами; Общие правила безопасной работы.

Практическая работа: Распознать ошибку в последовательности отправки документа.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 2. Ключи, сертификаты и носители — 4 ч.

Содержание: Ответственность владельца ключа; Хранение, использование и отзыв сертификатов; Действия при утрате или подозрении на компрометацию.

Практическая работа: Выбрать правильные действия в учебном сценарии утраты носителя.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 3. Практика защищённого обмена документами — 4 ч.

Содержание: Проверка адресата, вложения и подписи; Безопасный доступ к средствам документооборота; Работа с предупреждениями и сбоями.

Практическая работа: Разобрать пример проверки подписи и адресата.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 4. Инциденты и социальная инженерия — 3 ч.

Содержание: Фишинг и подмена реквизитов; Ошибки пользователя и каналы уведомления; Запрет передачи ключей и паролей.

Практическая работа: Составить краткое сообщение о подозрительном событии.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

6. Организационно-педагогические условия

Дистанционное обучение проводится с индивидуальным доступом к материалам и заданиям, консультациями преподавателя и фиксацией результатов проверки.

Занятия обеспечиваются специалистами, имеющими подготовку и практический опыт применения СКЗИ и защищённого документооборота.

Необходимы доступ в Интернет, электронные учебные материалы, демонстрационные сценарии и контрольные задания без реальных ключей и конфиденциальных документов.

Методическое обеспечение: памятки пользователей, инструкции, учебные кейсы и контрольные вопросы.

Актуализация программы проводится по мере изменения правил работы со СКЗИ и утверждается директором.

7. Контроль результатов и оценочные материалы

Текущий контроль проводится по заданиям модулей с результатом «зачтено/не зачтено». Слушатель получает комментарии к ошибкам и возможность повторного выполнения задания в пределах срока обучения.

Итоговый контроль: дистанционный тест и практико-ориентированный кейс. Тест содержит не менее 10 заданий по содержанию всех модулей. Для положительного результата требуется не менее 70% верных ответов и выполнение ключевых требований практического кейса. Допускается повторная проверка в порядке, предусмотренном локальными актами.

Типовые контрольные вопросы:

1. Можно ли передавать личный ключ электронной подписи коллеге?
2. Кому следует сообщить об утрате носителя?
3. Как проверить адресата защищённого электронного документа?
4. Что делать при подозрении на фишинговое письмо?
5. Что означает компрометация ключевой информации?

Практическое итоговое задание: Пользователь получил письмо с просьбой срочно передать ключ электронной подписи и подписать изменённый документ. Выберите правильный порядок действий.

Критерии оценки кейса: (1) корректно выделены исходные условия и риски; (2) действия и документы предложены последовательно; (3) применены уместные технические и организационные меры; (4) не предложены действия, противоречащие требованиям безопасности. Результат «зачтено» — выполнение не менее трёх из четырёх критериев при обязательном соблюдении критерия 4.

Результат обучения фиксируется в учётной ведомости. Удостоверение о повышении квалификации по настоящей программе не выдаётся.

8. Основные нормативные и методические источники

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
- Локальные инструкции организации по использованию СКЗИ и защищённого документооборота.

Учебные и справочные материалы актуализируются перед реализацией очередной группы с учётом действующих редакций нормативных документов.