7.1 Список курсов с описанием

Программа: Информационная безопасность банка

Папка	Кол-во курсов
Общие курсы	
Курсы по банковскому делу	
Курсы по информационной безопасности	
Демонстрационные курсы	2
Программы обучения для банков, применяющих положения СТО БР ИББС	
Базовые курсы	3
Обязательные программы обучения	15
Дополнительные и тематические программы обучения	4
Программы обучения для банков, НЕ применяющих положения СТО БР ИББС	
Базовые курсы	3
Обязательные программы обучения	5
Дополнительные и тематические программы обучения	12
Общее количество курсов:	**44**

N	Курс
Демонстрационные курсы	
1.764	**Демонстрационный курс "Законодательство в области информационной безопасности"** *Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с базовыми понятиями и терминами, необходимыми для понимания информационной безопасности, а также для ознакомления с общими мерами и принципами обеспечения информационной безопасности.* • Нормативно-правовые акты, затрагивающие вопросы информационной безопасности — 3 • Роль и виды стандартов информационной безопасности — 4 • Обзор базовых международных стандартов в области — 6

	информационной безопасности	
	• Заключение	2
	Всего вопросов	**15**
1.763	**Демонстрационный курс "Обучение пользователей в области информационной безопасности"** *Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014.*	
	• Понятие информационной безопасности. Основные термины и определения	4
	• Основные положения СТО БР ИББС-1.0-2014	5
	• Политика информационной безопасности	7
	• Обязанности работников по обеспечению информационной безопасности	3
	• Заключение	1
	Всего вопросов	**20**
Базовые курсы		
1.707	**Базовый курс "Понятие информационной безопасности и методы ее обеспечения"** *Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с базовыми понятиями и терминами, необходимыми для понимания информационной безопасности, а также для ознакомления с общими мерами и принципами обеспечения информационной безопасности.*	
	• Понятие и свойства информации	3
	• Понятие информационной безопасности. Методы обеспечения информационной безопасности	10
	• Информационная безопасность Российской Федерации в сфере экономики	5
	• Система информационной безопасности банка	6
	Всего вопросов	**24**

1.618 **Базовый курс "Законодательство в области информационной безопасности"**

Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с системой нормативно - правовых актов РФ, а также национальных и международных стандартов в области информационной безопасности.

• Нормативно-правовые акты, затрагивающие вопросы информационной безопасности	4
• Роль и виды стандартов информационной безопасности	9
• Обзор базовых международных стандартов в области информационной безопасности	7
Всего вопросов	**20**

1.619 **Базовый курс "Угрозы информационной безопасности"**

Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с понятиями уязвимостей, угроз информационной безопасности и их источников.

• Понятие и классификация угроз информационной безопасности	6
• Понятие и классификация уязвимостей информационной безопасности	5
• Понятие и классификация источников угроз информационной безопасности	6
• Модели угроз и нарушителей информационной безопасности	3
• Банк данных угроз безопасности информации	4
Всего вопросов	**24**

Обязательные программы обучения

1.791 **Общий курс по обучению пользователей в области информационной безопасности (СТО + ВБД) (для пользователей ИБС)**

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.8.9.1, п.8.9.4): - в организации БС РФ должна быть организована санкционированная руководством работа с персоналом в направлении повышения осведомленности и обучения в

области ИБ; - программы обучения и повышения осведомленности должны включать информацию: по существующим политикам ИБ, по применяемым в организации БС РФ защитным мерам, по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ, о значимости и важности деятельности работников для обеспечения ИБ организации БС РФ. Курс предназначен для обучения работников кредитной организации в области ИБ, в соответствии с указанными требованиями.

• Понятие информационной безопасности. Основные термины и определения	9
• Основные положения СТО БР ИББС-1.0-2014	16
• Политика информационной безопасности	22
• Обязанности работников по обеспечению информационной безопасности	11
Всего вопросов	**58**

1.746

Курс по повышению осведомленности пользователей в области информационной безопасности: Изменения законодательства, технологий защиты, активности ВК (НД + прочие источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.8.9.1, п.8.9.4): - в организации БС РФ должна быть организована санкционированная руководством работа с персоналом в направлении повышения осведомленности и обучения в области ИБ; - программы обучения и повышения осведомленности должны включать информацию: по существующим политикам ИБ, по применяемым в организации БС РФ защитным мерам, по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ, о значимости и важности деятельности работников для обеспечения ИБ организации БС РФ. Курс предназначен для повышения осведомленности работников кредитной организации в области информационной безопасности, в соответствии с указанными требованиями.

• Изменения законодательства в области информационной безопасности	12
• Системы ДБО: Развитие технологий защиты	10
• Понятие вредоносного ПО. Статистика по вредоносным программам в 2015 г.	3
• Обзор новых вредоносных программ 2016 г.	11

	Всего вопросов	**36**

1.719 **Общий курс по защите информации при осуществлении переводов денежных средств (382-П+552-П+ПНД+ВБД) (для специалистов)**

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основу курса положены требования Положения Банка России от 09.06.2012 N 382-П. Курс предназначен для ПОВЫШЕНИЯ ОСВЕДОМЛЕНОСТИ специалистов по тематике защиты информации при осуществлении переводов денежных средств, в соответствии с п.п.2.12.1 - 2.12.3 Положения N 382-П, п.9.1 Положения N 552-П.

• 1. Общие положения о защите информации	7
• 2. Защищаемая информация. Общие требования к защите информации при осуществлении переводов денежных средств	4
• 3. Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств	4
• 3.1 Порядок информирования Банка России о выявленных инцидентах и хранению информации об инцидентах	2
• 4. Организационные меры защиты информации при осуществлении переводов денежных средств	2
• 5. Технические средства защиты информации при осуществлении переводов денежных средств	3
• 6. Порядок применения отдельных мер защиты информации при осуществлении переводов денежных средств	8
• 6.1. Порядок защиты информации при осуществлении переводов денежных средств с использованием СКЗИ	8
• 6.2. Порядок защиты информации при осуществлении переводов денежных средств с использованием сети Интернет	13
• 6.3. Порядок защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов	5
Всего вопросов	**56**

1.737 **Общий курс по защите от вредоносного кода (49-Т+ПНД+ВБД) (для пользователей ИБС)**

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса - требования письма Банка России от 24.03.2014 N 49-Т. Курс предназначен для проведения обучения работников кредитной организации по тематике

защиты от вредоносного кода, в соответствии с п.2.1.3 указанного письма.

• Понятие и условия существования вредоносного кода	8
• Общие правила работы пользователей в ИБС	4
• Общие правила работы пользователей в сети Интернет и с корпоративной электронной почтой	2
• Обязанности персонала банка по защите от вредоносного кода	4
• Мероприятия банка в части обеспечения защиты от вредоносного кода	7
Всего вопросов	**25**

1.739

Курс по организации защиты от вредоносного кода (49-Т+ПНД+ВБД) (для органов управления банка)

Курс разработан для органов управления кредитных организаций. В основе курса - требования письма Банка России от 24.03.2014 N 49-Т. Курс предназначен для проведения обучающих мероприятий по тематике организации защиты от вредоносного кода, в соответствии с п.2.1.3 и р.3 указанного письма.

• Понятие и условия существования вредоносного кода	8
• Мероприятия банка в части обеспечения защиты от вредоносного кода	6
• Организация использования сети Интернет	4
• Организация защиты от вредоносного кода	4
• Организация работы сотрудников по защите от вредоносного кода	4
Всего вопросов	**26**

1.740

Курс по защите от вредоносного кода клиентов банка - пользователей систем ДБО (ВБД+прочие источники) (для специалистов банка)

Курс разработан для специалистов кредитных организаций, осуществляющих консультирование клиентов по вопросам защиты от вредоносного кода. В основе курса требования письма Банка России от 24.03.2014 N 49-Т (п.2.1.5, п.4.2.6, п.4.2.7 и п.4.3): - регулярный сбор и анализ информации о распространении ВК; - консультирование клиентов - пользователей систем ДБО по вопросам защиты от ВК на постоянной основе; - информирование клиентов - пользователей систем ДБО кредитной организации о новых разновидностях ВК, угрожающих безопасности клиентских АРМ систем ДБО, способах защиты от их воздействия; - подготовку и переподготовку работников кредитной организации, ответственных за работу с клиентами - пользователями систем ДБО. Курс

	предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями. • Атаки на системы ДБО — 6 • Понятие и виды вредоносного ПО — 13 • Обзор новых вредоносных программ 2015 г., 2016 г. — 9 • Банковские вредоносные программы — 8 • Мероприятия банка по защите от вредоносного кода систем ДБО — 2 • Требования к клиентам по защите от вредоносного кода клиентских АРМ систем ДБО — 4 Всего вопросов — **42**
1.761	**Курс по защите от вредоносного кода клиентов банка - пользователей систем ДБО (ВБД+прочие источники) (для клиентов)** *Курс разработан для клиентов кредитных организаций - пользователей систем ДБО в целях информирования последних по вопросам защиты от вредоносного кода, в соответствии с требованиями п.4.2.6, п.4.2.7 письма Банка России от 24.03.2014 N 49-Т.* • Понятие системы ДБО. Атаки на системы ДБО — 8 • Понятие и виды вредоносного ПО — 13 • Обзор новых вредоносных программ 2015 г., 2016 г. — 10 • Банковские вредоносные программы — 8 • Требования и рекомендации клиентам по защите от вредоносного кода клиентских АРМ систем ДБО — 8 Всего вопросов — **47**
1.745	**Общий курс по обучению в области обработки и обеспечения безопасности персональных данных (СТО+ ПНД+ ВБД) (для специалистов)** *Курс разработан для специалистов кредитных организаций, осуществляющих обработку персональных данных. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.7.10.7): - в организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры ознакомления работников организации БС РФ, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами организации БС РФ*

содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей; - организация БС РФ может проводить указанное ознакомление работников в ходе проведения мероприятий по их обучению или повышению осведомленности. Курс предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями.

• Нормативные документы. Основные понятия	3
• Принципы и условия обработки персональных данных	8
• Контроль и надзор за обработкой персональных данных	3
• Обязанности и права должностных лиц при обработке персональных данных	2
• Общие положения о защите персональных данных	8
• Угрозы безопасности ПДн и уровни защищенности ПДн при их обработке	7
• Мероприятия банка по обеспечению безопасности персональных данных	2
• Обязанности, права и ответственность должностных лиц по обеспечению безопасности персональных данных	4
Всего вопросов	**37**

1.777

Курс по повышению осведомленности в области обработки и обеспечения безопасности персональных данных (СТО+ПНД+ ВБД) (для специалистов)

Курс разработан для специалистов кредитных организаций, осуществляющих обработку персональных данных. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.7.10.7): - в организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры ознакомления работников организации БС РФ, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами организации БС РФ, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей; - организация БС РФ может проводить указанное ознакомление работников в ходе проведения мероприятий по их обучению или повышению осведомленности. Курс предназначен для повышения осведомленности работников в области обработки и обеспечения безопасности персональных данных, в соответствии с указанными требованиями.

• Нормативные документы. Основные понятия	6

• Принципы и условия обработки персональных данных	15
• Обязанности и права должностных лиц при обработке персональных данных	6
• Угрозы безопасности ПДн и уровни защищенности ПДн при их обработке	6
• Состав и содержание мер по обеспечению безопасности персональных данных	5
• Контроль и надзор за обеспечением безопасности персональных данных	2
• Мероприятия банка по обеспечению безопасности персональных данных	11
• Обязанности и права должностных лиц по обеспечению безопасности персональных данных	5
Всего вопросов	**56**

1.766

Общий курс по обучению в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ (СТО + ВБД) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" РС БР ИББС-2.5-2014 (п.5.3): - реализация в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий: проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Курс предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями.

• Общие сведения об инцидентах ИБ. Понятия и термины.	7
• Признаки нарушения ИБ	6
• Обработка инцидентов ИБ	7
• Мероприятия банка по реагированию на инциденты ИБ	6
• Обязанности должностных лиц при обнаружении и реагировании на инциденты ИБ	4

	Всего вопросов	**30**

1.742

Курс по повышению осведомленности в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ (СТО + ВБД) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" РС БР ИББС-2.5-2014 (п.5.3): - реализация в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий: проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Курс предназначен для повышения осведомленности работников в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ, в соответствии с указанными требованиями.

• Основные сведения об инцидентах ИБ. Понятия и термины.	7
• Менеджмент инцидентов ИБ: общие понятия и нормативные документы	3
• Планирование в рамках системы менеджмента инцидентов ИБ	4
• Реализация и анализ в рамках системы менеджмента инцидентов ИБ	8
• Обнаружение и классификация инцидентов ИБ	11
• Мероприятия банка по реагированию на инциденты ИБ	6
• Обязанности должностных лиц при обнаружении и реагировании на инциденты ИБ	10
Всего вопросов	**49**

1.767

Курс по обучению в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ (ПНД+прочие источники) (для клиентов)

Курс разработан для обучения и повышения осведомленности КЛИЕНТОВ БАНКА в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка. В основе курса требования Рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" РС БР ИББС-2.5-2014 (п.5.3): - реализация

в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий: проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Курс разработан для клиентов кредитных организаций в целях информирования последних по вопросам обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка, в соответствии с указанными требованиями.

• Инциденты ИБ и законодательство РФ	5
• Общий порядок реагирования на инцидент ИБ	6
• Признаки инцидента ИБ в системе ДБО	6
• Инструкция для клиента банка в случае инцидента ИБ в системе ДБО	4
• Признаки инцидента ИБ при работе с платежными картами	10
• Инструкция для клиента банка в случае инцидента ИБ с платежными картами	2
Всего вопросов	**33**

1.768

Курс по обучению в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ (ПНД+прочие источники) (для представителей внешних организаций)

Курс разработан для обучения и повышения осведомленности представителей внешних организаций в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка. В основе курса требования Рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" РС БР ИББС-2.5-2014 (п.5.3): - реализация в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий: проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Курс разработан для представителей внешних организаций в целях информирования последних по вопросам обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка в соответствии с указанными требованиями.

• Инциденты ИБ и законодательство РФ	3
• Инциденты, связанные с нарушением требований к	4

	обеспечению защиты информации при осуществлении переводов денежных средств	
	• Инциденты, связанные с нарушением требований к обеспечению защиты информации при обслуживании банкоматов	3
	• Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении платежей через интернет	3
	• Общий алгоритм действий при наступлении инцидента ИБ	4
	• Реагирование на инцидент ИБ	8
	• Обязанности должностных лиц при обнаружении и реагировании на инцидент ИБ	3
	Всего вопросов	**28**

1.769

Общий курс по обучению в области обеспечения непрерывности бизнеса и его восстановления после прерываний (СТО+ПНД+ВБД) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.8.11.8): - в организации БС РФ должна быть реализована программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний Курс предназначен для обучения работников кредитной организации, в соответствии с указанными требованиями.

• Менеджмент непрерывности бизнеса: общие понятия и нормативные документы	4
• Требования к разработке и тестированию плана ОНиВД	10
• Мероприятия банка по обеспечению непрерывности бизнеса и восстановлению деятельности после прерываний	4
• Действия ответственных лиц при возникновении внештатных ситуаций	2
Всего вопросов	**20**

1.778

Курс по повышению осведомленности в области обеспечения непрерывности бизнеса и его восстановления после прерываний (СТО+ПНД+ВБД) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций -

пользователей информационной банковской системы. В основе курса требования Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения"СТО БР ИББС-1.0-2014 (п.8.11.8): - в организации БС РФ должна быть реализована программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний Курс предназначен для повышения осведомленности работников кредитной организации, в соответствии с указанными требованиями.

• Менеджмент непрерывности бизнеса: общие понятия и нормативные документы	8
• Требования к разработке и тестированию плана ОНиВД	6
• Мероприятия банка по обеспечению непрерывности бизнеса и восстановлению деятельности после прерываний	8
• Действия ответственных лиц при возникновении внештатных ситуаций	5
Всего вопросов	**27**

Дополнительные и тематические программы обучения

1.841

Тематический курс "Коммерческая тайна"

Курс разработан для всех категорий специалистов кредитной организации. Курс предназначен для ознакомления работников с основными положениями закона от 29.07.2004 г. N 98-ФЗ "О коммерческой тайне", а также обязанностями работников по охране конфиденциальности информации, составляющей коммерческую тайну, и мерами ответственности за разглашение указанной информации.

• Термины и определения. Нормативные документы	9
• Меры по охране конфиденциальности информации	13
• Конфиденциальность информации, составляющей коммерческую тайну, в рамках трудовых отношений	9
• Ответственность за разглашение информации, составляющей коммерческую тайну	8
Всего вопросов	**39**

1.749

Дополнительный курс "Вредоносное ПО. Средства защиты от вредоносного ПО"

Курс разработан для работников кредитной организации - пользователей ИБС, имеющих общее представление об антивирусных технологиях, но не являющихся специалистами в области защиты от вредоносных программ. Курс предназначен для расширения и систематизации знаний работников

кредитной организации в области вредоносных программ и средств защиты от них.

• Понятие и условия существования вредоносных программ	5
• Виды вредоносных программ	15
• Понятие и виды антивирусных программ. Прочие средства защиты от вредоносного ПО	14
• Технологии обнаружения вредоносного кода	11
Всего вопросов	**45**

1.1020 **Курс для подготовки к тесту "Меры безопасного использования электронных средств платежа"**

• Общие вопросы использования ЭСП	10
• Защита информации при осуществлении переводов денежных средств	10
• Коммерческая и банковская тайна	10
• Способы мошенничества при использовании ЭСП	10
• Меры безопасного использования ЭСП клиентами и сотрудниками банка	10
Всего вопросов	**50**

1.1014 **Тематический курс "Социальная инженерия как вид мошенничества: виды атак и способы противодействия"**

Сегодня человеческий фактор в информационной безопасности играет очень важную роль. Проблему информационной безопасностиуже нельзя решить просто с помощью аппаратных и программных средств. Технологии безопасности, которым все привыкли доверять, – межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и другие – малоэффективны в противостоянии хакерам, использующим методы социальной инженерии. Необходима работа с персоналом, обучение сотрудников применению политики безопасности и техникам противостояния социоинженерам. Курс разработан для работников кредитной организации - пользователей ИБС, имеющих общее представление об информационной безопасности организации, но не являющихся специалистами в данной области. Курс предназначен для повышения осведомленности работников кредитной организации - пользователей ИБС в области информационной безопасности.

• Общие сведения о социальной инженерии, как виде мошенничества	7
• Краткая характеристики основных видов атак, совершаемых с	10

использованием методов социальной инженерии	
• Примеры атак, совершаемых с использованием методов социальной инжененнрии	7
• Основные правила поведения сотрудников с целью противодействия возможным атакам социальных инженеров	6
Всего вопросов	**30**

Базовые курсы

1.939 **Базовый курс "Понятие информационной безопасности и методы ее обеспечения"**

Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с базовыми понятиями и терминами, необходимыми для понимания информационной безопасности, а также для ознакомления с общими мерами и принципами обеспечения информационной безопасности.

• Понятие и свойства информации	3
• Понятие информационной безопасности. Методы обеспечения информационной безопасности	10
• Информационная безопасность Российской Федерации в сфере экономики	5
• Информационная безопасность организации	6
Всего вопросов	**24**

1.940 **Базовый курс "Законодательство в области информационной безопасности"**

Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с системой нормативно - правовых актов РФ, а также национальных и международных стандартов в области информационной безопасности.

• Нормативно-правовые акты, затрагивающие вопросы информационной безопасности	4
• Роль и виды стандартов информационной безопасности	8
• Обзор базовых международных стандартов в области информационной безопасности	7
Всего вопросов	**19**

1.941

Базовый курс "Угрозы информационной безопасности"

Курс разработан для специалистов кредитных организаций - пользователей информационной банковской системы. Курс предназначен для ознакомления работников с понятиями уязвимостей, угроз информационной безопасности и их источников.

• Понятие и классификация угроз информационной безопасности	6
• Понятие и классификация уязвимостей информационной безопасности	5
• Понятие и классификация источников угроз информационной безопасности	2
• Модель угроз информационной безопасности	3
• Банк данных угроз безопасности информации	4
Всего вопросов	**20**

Обязательные программы обучения

1.934

Общий курс по защите информации при осуществлении переводов денежных средств (382-П+552-П+ПНД+ВБД) (для специалистов)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основу курса положены требования Положения Банка России от 09.06.2012 N 382-П. Курс предназначен для ПОВЫШЕНИЯ ОСВЕДОМЛЕНОСТИ специалистов по тематике защиты информации при осуществлении переводов денежных средств, в соответствии с п.п.2.12.1 - 2.12.3 Положения N 382-П.

• 1. Общие положения о защите информации	7
• 2. Защищаемая информация. Общие требования к защите информации при осуществлении переводов денежных средств	4
• 3. Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств	4
• 3.1 Порядок информирования Банка России о выявленных инцидентах и хранению информации об инцидентах	2
• 4. Порядок применения отдельных мер защиты информации при осуществлении переводов денежных средств	7
• 4.1. Порядок защиты информации при осуществлении переводов денежных средств с использованием СКЗИ	8
• 4.2. Порядок защиты информации при осуществлении переводов денежных средств с использованием сети Интернет	13

	• 4.3. Порядок защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов	7
	Всего вопросов	**52**
1.935	**Общий курс по защите от вредоносного кода (49-Т+ПНД+ВБД) (для пользователей ИБС)** *Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса - требования письма Банка России от 24.03.2014 N 49-Т. Курс предназначен для проведения обучения работников кредитной организации по тематике защиты от вредоносного кода, в соответствии с п.2.1.3 указанного письма.*	
	• Понятие и условия существования вредоносного кода	7
	• Общие правила работы пользователей в ИБС	4
	• Общие правила работы пользователей в сети Интернет и с корпоративной электронной почтой	2
	• Обязанности персонала банка по защите от вредоносного кода	4
	• Мероприятия банка в части обеспечения защиты от вредоносного кода	7
	Всего вопросов	**24**
1.936	**Курс по организации защиты от вредоносного кода (49-Т+ПНД+ВБД) (для органов управления банка)** *Курс разработан для органов управления кредитных организаций. В основе курса - требования письма Банка России от 24.03.2014 N 49-Т. Курс предназначен для проведения обучающих мероприятий по тематике организации защиты от вредоносного кода, в соответствии с п.2.1.3 и р.3 указанного письма.*	
	• Понятие и условия существования вредоносного кода	7
	• Мероприятия банка в части обеспечения защиты от вредоносного кода	6
	• Организация защиты от вредоносного кода	4
	• Организация работы сотрудников по защите от вредоносного кода	4
	Всего вопросов	**21**
1.937	**Курс по защите от вредоносного кода клиентов банка - пользователей систем ДБО (ВБД+прочие источники) (для специалистов банка)**	

Курс разработан для специалистов кредитных организаций, осуществляющих консультирование клиентов по вопросам защиты от вредоносного кода. В основе курса требования письма Банка России от 24.03.2014 N 49-Т (п.2.1.5, п.4.2.6, п.4.2.7 и п.4.3): - регулярный сбор и анализ информации о распространении ВК; - консультирование клиентов - пользователей систем ДБО по вопросам защиты от ВК на постоянной основе; - информирование клиентов - пользователей систем ДБО кредитной организации о новых разновидностях ВК, угрожающих безопасности клиентских АРМ систем ДБО, способах защиты от их воздействия; - подготовку и переподготовку работников кредитной организации, ответственных за работу с клиентами - пользователями систем ДБО. Курс предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями.

• Атаки на системы ДБО	5
• Понятие и виды вредоносного ПО	13
• Обзор новых вредоносных программ 2015 г., 2016 г.	10
• Банковские вредоносные программы	8
• Мероприятия банка по защите от вредоносного кода систем ДБО	2
• Требования к клиентам по защите от вредоносного кода клиентских АРМ систем ДБО	4
Всего вопросов	**42**

1.938

Курс по защите от вредоносного кода клиентов банка - пользователей систем ДБО (ВБД+прочие источники) (для клиентов)

Курс разработан для клиентов кредитных организаций - пользователей систем ДБО в целях информирования последних по вопросам защиты от вредоносного кода, в соответствии с требованиями п.4.2.6, п.4.2.7 письма Банка России от 24.03.2014 N 49-Т.

• Понятие системы ДБО. Атаки на системы ДБО	8
• Понятие и виды вредоносного ПО	13
• Обзор новых вредоносных программ 2015 г., 2016 г.	10
• Банковские вредоносные программы	8
• Требования и рекомендации клиентам по защите от вредоносного кода клиентских АРМ систем ДБО	8
Всего вопросов	**47**

Дополнительные и тематические программы обучения

1.942

Тематический курс "Обучение пользователей в области информационной безопасности" (НД + ВБД + прочие источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования ГОСТ Р ИСО/МЭК 27002-2012. В соответствии с указанным стандартом, к мерам и средствам контроля и управления безопасностью относится, в числе прочих, и безопасность, связанная с персоналом (п.8.2.2): Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их рабочих функций. Курс предназначен для обучения работников кредитной организации в области ИБ, в соответствии с указанными требованиями.

• Понятие информационной безопасности. Основные термины и определения	8
• Политика информационной безопасности	19
• Обязанности работников по обеспечению информационной безопасности	11
Всего вопросов	**38**

1.943

Дополнительный курс "Повышение осведомленности пользователей в области ИБ: Изменения законодательства, технологий защиты, активности ВК" (НД + прочие источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования ГОСТ Р ИСО/МЭК 27002-2012. В соответствии с указанным стандартом, к мерам и средствам контроля и управления безопасностью относится, в числе прочих, и безопасность, связанная с персоналом (п.8.2.2): Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их рабочих функций. Курс предназначен для повышения осведомленности работников кредитной организации в области информационной безопасности, в соответствии с указанными требованиями.

• Изменения законодательства в области информационной безопасности	11
• Системы ДБО: Развитие технологий защиты	10
• Понятие вредоносного ПО. Статистика по вредоносным программам в 2015 г.	3
• Обзор новых вредоносных программ 2016 г.	11

Всего вопросов	**35**

1.944

Тематический курс "Обучение в области обработки и обеспечения безопасности персональных данных" (НД + ВБД + прочие источники) (для специалистов)

Курс разработан для специалистов кредитных организаций, осуществляющих обработку персональных данных. В основе курса требования федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"(ст.18.1 п.1 п.п.6): Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных". Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных указанным федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться: - ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников. Курс предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями.

• Нормативные документы. Основные понятия	3
• Принципы и условия обработки персональных данных	8
• Контроль и надзор за обработкой персональных данных	3
• Обязанности и права должностных лиц при обработке персональных данных	2
• Общие положения о защите персональных данных	8
• Угрозы безопасности ПДн и уровни защищенности ПДн при их обработке	7
• Мероприятия банка по обеспечению безопасности персональных данных	1
• Обязанности, права и ответственность должностных лиц по обеспечению безопасности персональных данных	4
Всего вопросов	**36**

1.945 **Дополнительный курс "Повышение осведомленности в области**

обработки и обеспечения безопасности персональных данных" (НД + ВБД + прочие источники) (для специалистов)

Курс разработан для специалистов кредитных организаций, осуществляющих обработку персональных данных. В основе курса требования федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (ст.18.1 п.1 п.п.6): Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных". Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных указанным федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться: - ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников. Курс предназначен для повышения осведомленности работников в области обработки и обеспечения безопасности персональных данных, в соответствии с указанными требованиями.

• Нормативные документы. Основные понятия	6
• Принципы и условия обработки персональных данных	15
• Обязанности и права должностных лиц при обработке персональных данных	6
• Угрозы безопасности ПДн и уровни защищенности ПДн при их обработке	6
• Состав и содержание мер по обеспечению безопасности персональных данных	5
• Контроль и надзор за обеспечением безопасности персональных данных	2
• Мероприятия банка по обеспечению безопасности персональных данных	10
• Обязанности и права должностных лиц по обеспечению безопасности персональных данных	5
Всего вопросов	**55**

1.946 **Тематический курс "Обучение в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ" (НД + ВБД + прочие**

источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования национального стандарта РФ ГОСТ Р ИСО/МЭК 18044-2007 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. (п.7.7 Обеспечение осведомленности и обучение): Менеджмент инцидентов ИБ – это процесс, который включает в себя не только технические средства, но также и людей, и, следовательно, этот процесс должен поддерживаться людьми, соответствующим образом обученными для работы в организации и ос- ведомленными в вопросах безопасности информации. Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту инцидентов ИБ. Поэтому роль менеджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков. Курс предназначен для подготовки и переподготовки работников кредитной организации, в соответствии с указанными требованиями.

• Общие сведения об инцидентах ИБ. Понятия и термины.	4
• Примеры инцидентов ИБ и их причин	8
• Обработка событий и инцидентов ИБ	4
• Управление инцидентами ИБ	5
• Обязанности должностных лиц по реагированию на инциденты ИБ	6
Всего вопросов	**27**

1.947

Дополнительный курс "Повышение осведомленности в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ" (НД + ВБД + прочие источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования национального стандарта РФ ГОСТ Р ИСО/МЭК 18044-2007 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. (п.7.7 Обеспечение осведомленности и обучение): Менеджмент инцидентов ИБ – это процесс, который включает в себя не только технические средства, но также и людей, и, следовательно, этот процесс должен поддерживаться людьми, соответствующим образом обученными для работы в организации и ос- ведомленными в вопросах безопасности информации. Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту

инцидентов ИБ. Поэтому роль менеджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков. Курс предназначен для повышения осведомленности работников в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ, в соответствии с указанными требованиями. области обнаружения инцидентов ИБ и реагирования на инциденты ИБ, в соответствии с указанными требованиями.

• Основные сведения об инцидентах ИБ. Понятия и термины.	6
• Менеджмент инцидентов ИБ: общие понятия и документы	4
• Этап "Планирование и подготовка" в рамках системы менеджмента инцидентов ИБ	4
• Этап "Использование" в рамках системы менеджмента инцидентов ИБ	8
• Этап "Анализ" в рамках системы менеджмента инцидентов ИБ	2
• Этап "Улучшение" в рамках системы менеджмента инцидентов ИБ	2
• Обязанности должностных лиц при обнаружении и реагировании на инциденты ИБ	7
Всего вопросов	**33**

1.948

Тематический курс "Обучение в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ" (НД + прочие источники) (для клиентов)

Курс разработан для обучения и повышения осведомленности КЛИЕНТОВ БАНКА в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка. В основе курса требования национального стандарта РФ ГОСТ Р ИСО/МЭК 18044-2007 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. (п.7.7 Обеспечение осведомленности и обучение): Менеджмент инцидентов ИБ – это процесс, который включает в себя не только технические средства, но также и людей, и, следовательно, этот процесс должен поддерживаться людьми, соответствующим образом обученными для работы в организации и ос- ведомленными в вопросах безопасности информации. Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту инцидентов ИБ. Поэтому роль менеджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала

включая новых служащих, пользователей сторонних организаций и подрядчиков. Курс разработан для клиентов кредитных организаций в целях информирования последних по вопросам обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка, в соответствии с указанными требованиями.

• Инциденты ИБ и законодательство РФ	5
• Общий порядок реагирования на инцидент ИБ	6
• Признаки инцидента ИБ в системе ДБО	6
• Инструкция для клиента банка в случае инцидента ИБ в системе ДБО	4
• Признаки инцидента ИБ при работе с платежными картами	10
• Инструкция для клиента банка в случае инцидента ИБ с платежными картами	2
Всего вопросов	**33**

1.949

Тематический курс "Обучение в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ" (НД + прочие источники) (для представителей внешних организаций)

Курс разработан для обучения и повышения осведомленности представителей внешних организаций в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка. В основе курса требования национального стандарта РФ ГОСТ Р ИСО/МЭК 18044-2007 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. (п.7.7 Обеспечение осведомленности и обучение): Менеджмент инцидентов ИБ – это процесс, который включает в себя не только технические средства, но также и людей, и, следовательно, этот процесс должен поддерживаться людьми, соответствующим образом обученными для работы в организации и ос- ведомленными в вопросах безопасности информации. Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту инцидентов ИБ. Поэтому роль менеджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков. Курс разработан для представителей внешних организаций в целях информирования последних по вопросам обнаружения инцидентов ИБ и реагирования на инциденты ИБ при использовании информационной инфраструктуры банка в соответствии с указанными требованиями.

• Инциденты ИБ и законодательство РФ	4

	• Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств	4
	• Инциденты, связанные с нарушением требований к обеспечению защиты информации при обслуживании банкоматов	3
	• Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении платежей через интернет	3
	• Общий алгоритм действий при наступлении инцидента ИБ	4
	• Реагирование на инцидент ИБ	4
	• Обязанности должностных лиц при обнаружении и реагировании на инцидент ИБ	3
	Всего вопросов	**25**
1.950	**Тематический курс "Обучение в области обеспечения непрерывности бизнеса и его восстановления после прерываний" (НД + ВБД + прочие источники) (для пользователей ИБС)** *Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 53647.1-229, ГОСТ Р 53647.2-2009. В соответствии с ГОСТ Р ИСО/МЭК 27002-2012, к мерам и средствам контроля и управления безопасностью относится, в числе прочих, и менеджмент непрерывности бизнеса (п.3.1, j): - при разработке и внедрении планов обеспечения непрерывности бизнеса, учитывающих информационную безопасность, следует предусмотреть соответствующее обучение сотрудников согласованным процедурам и процессам, включая управление в критических ситуациях (п.14.1.3. f); - в основу планирования непрерывности бизнеса должны быть заложены требования информационной безопасности, и предусмотрено информирование, обучение и тренинг, направленные на понимание процессов обеспечения непрерывности бизнеса и обеспечение уверенности в эффективности этих процессов (п.14.1.4 g). В соответствии с ГОСТ Р 53647.1-2009 деятельность по выполнению программы непрерывности бизнеса должна включать организацию и/или обеспечение соответствующего обучения персонала (п.5.3.1). В соответствии с ГОСТ Р 53647.2-2009 организация должна развивать, повышать и поддерживать осведомленность всего персонала путем непрерывного обучения и создания информационных программ в области менеджмента непрерывности бизнеса (п.3.3 a). Курс предназначен для обучения работников кредитной организации, в соответствии с указанными требованиями.*	
	• Менеджмент непрерывности бизнеса: общие понятия и нормативные документы	5

• Требования к разработке и тестированию плана ОНиВД	8
• Мероприятия банка по обеспечению непрерывности бизнеса и восстановлению деятельности после прерываний	6
• Действия ответственных лиц при возникновении внештатных ситуаций	2
Всего вопросов	**21**

1.951

Дополнительный курс "Повышение осведомленности в области обеспечения непрерывности бизнеса и его восстановления после прерываний" (НД + ВБД + прочие источники) (для пользователей ИБС)

Курс разработан для всех категорий специалистов кредитных организаций - пользователей информационной банковской системы. В основе курса требования ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р 53647.1-229, ГОСТ Р 53647.2-2009. В соответствии с ГОСТ Р ИСО/МЭК 27002-2012, к мерам и средствам контроля и управления безопасностью относится, в числе прочих, и менеджмент непрерывности бизнеса (п.3.1, j): - при разработке и внедрении планов обеспечения непрерывности бизнеса, учитывающих информационную безопасность, следует предусмотреть соответствующее обучение сотрудников согласованным процедурам и процессам, включая управление в критических ситуациях (п.14.1.3. f); - в основу планирования непрерывности бизнеса должны быть заложены требования информационной безопасности, и предусмотрено информирование, обучение и тренинг, направленные на понимание процессов обеспечения непрерывности бизнеса и обеспечение уверенности в эффективности этих процессов (п.14.1.4 g). В соответствии с ГОСТ Р 53647.1-2009 деятельность по выполнению программы непрерывности бизнеса должна включать организацию и/или обеспечение соответствующего обучения персонала (п.5.3.1). В соответствии с ГОСТ Р 53647.2-2009 организация должна развивать, повышать и поддерживать осведомленность всего персонала путем непрерывного обучения и создания информационных программ в области менеджмента непрерывности бизнеса (п.3.3 a). Курс предназначен для повышения осведомленности работников кредитной организации, в соответствии с указанными требованиями.

• Менеджмент непрерывности бизнеса: общие понятия и нормативные документы	8
• Требования к разработке и тестированию плана ОНиВД	6
• Мероприятия банка по обеспечению непрерывности бизнеса и восстановлению деятельности после прерываний	8
• Действия ответственных лиц при возникновении внештатных ситуаций	5
Всего вопросов	**27**

1.952 **Тематический курс "Коммерческая тайна"**

Курс разработан для всех категорий специалистов кредитной организации. Курс предназначен для ознакомления работников с основными положениями закона от 29.07.2004 г. N 98-ФЗ "О коммерческой тайне", а также обязанностями работников по охране конфиденциальности информации, составляющей коммерческую тайну, и мерами ответственности за разглашение указанной информации.

• Термины и определения. Нормативные документы	9
• Меры по охране конфиденциальности информации	13
• Конфиденциальность информации, составляющей коммерческую тайну, в рамках трудовых отношений	9
• Ответственность за разглашение информации, составляющей коммерческую тайну	8
Всего вопросов	**39**

1.953 **Дополнительный курс "Вредоносное ПО. Средства защиты от вредоносного ПО"**

Курс разработан для работников кредитной организации - пользователей ИБС, имеющих общее представление об антивирусных технологиях, но не являющихся специалистами в области защиты от вредоносных программ. Курс предназначен для расширения и систематизации знаний работников кредитной организации в области вредоносных программ и средств защиты от них.

• Понятие и условия существования вредоносных программ	5
• Виды вредоносных программ	15
• Понятие и виды антивирусных программ. Прочие средства защиты от вредоносного ПО	14
• Технологии обнаружения вредоносного кода	11
Всего вопросов	**45**