

Эффективная защита персональных данных через обучение сотрудников.

Современное законодательство и требования к специалистам.

Спикер: Эльшан Мамедов

Преподаватель Академии Softline, эксперт по защите информации, кандидат юридических наук

Через обучение - к успеху!
Знания работают на вас



Мамедов Эльшан
(Кандидат юридических наук)

ПРОФЕССИОНАЛЬНЫЙ ОПЫТ:

- ▶ Преподаватель-эксперт **Академии Softline**
- ▶ Доцент Центра компетенций по кибербезопасности ФГБОУ ВО ИРНИТУ
- ▶ Руководитель основной образовательной программы «информационная безопасность» ФГБОУ ВО ИРНИТУ
- ▶ Начальник отдела контрольно-ревизионной деятельности и профилактики правонарушений Департамента комплексной безопасности федерального госучреждения
- ▶ Эксперт-методолог по обработке и защите персональных данных (DPO) консалтинговой компании
- ▶ Внешний DPO крупной энергетической компании
- ▶ Стаж работы в госсекторе – 15 лет

Основные факты об утечках ПДн в 2023-2024 годах

2024

- В России утечек информации стало больше на **10%**

■ Утечки информации сократились за счет снижения количества зарегистрированных инцидентов в США

- Количество утекших записей персональных данных в России за I полугодие составило почти **1 млрд**

- Крупных баз в первом полугодии 2024 года утекло **на треть меньше**, чем в первом полугодии 2023 года

■ На одну утечку информации в мире. В среднем приходится **2,52** млн записей ПДн, в России – **2,38 млн**

- Доля **умышленных нарушений** среди утечек информации в России составила более **99%**

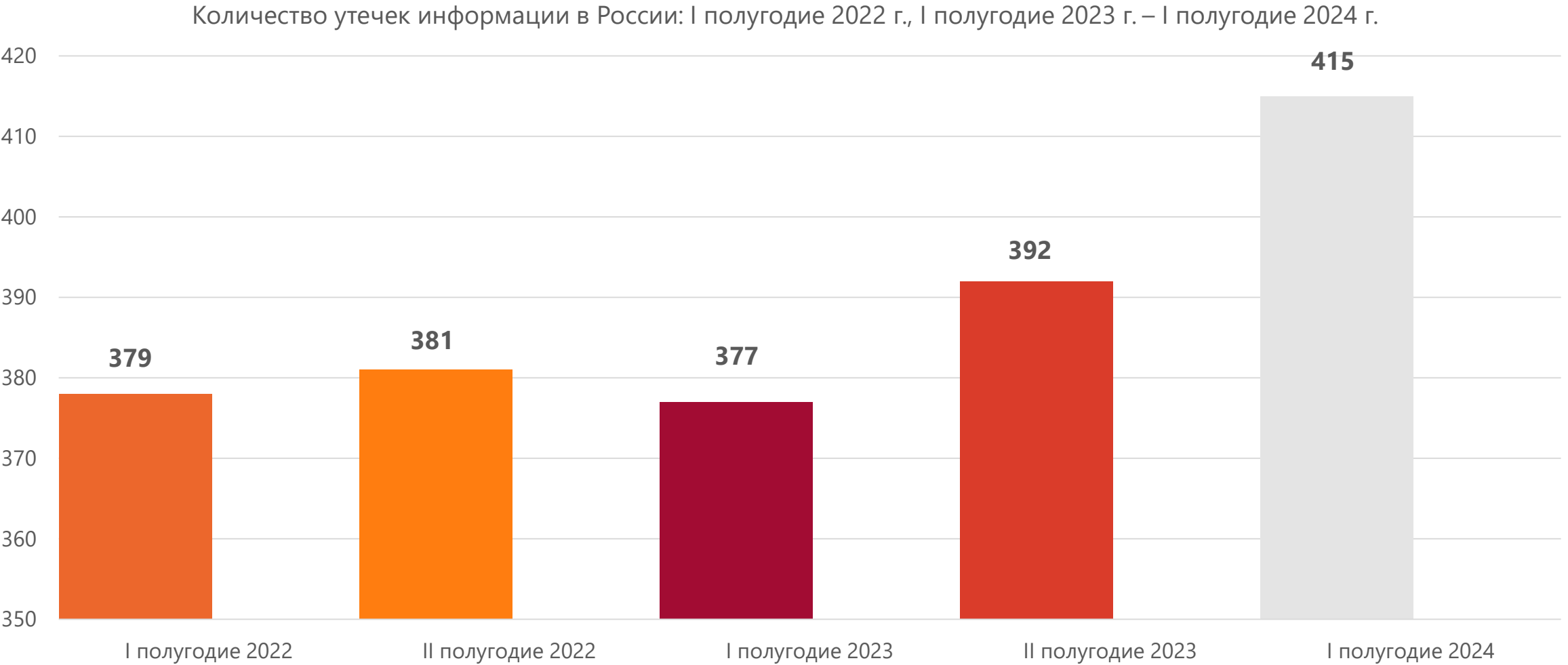
- В I полугодии 2024 года заметно **выросли доли утечек** в торговле промышленности

■ В России почти **вдвое выросла доля утечек** гостайны

- Более **половины утечек** информации в России случились в сфере **малого бизнеса**

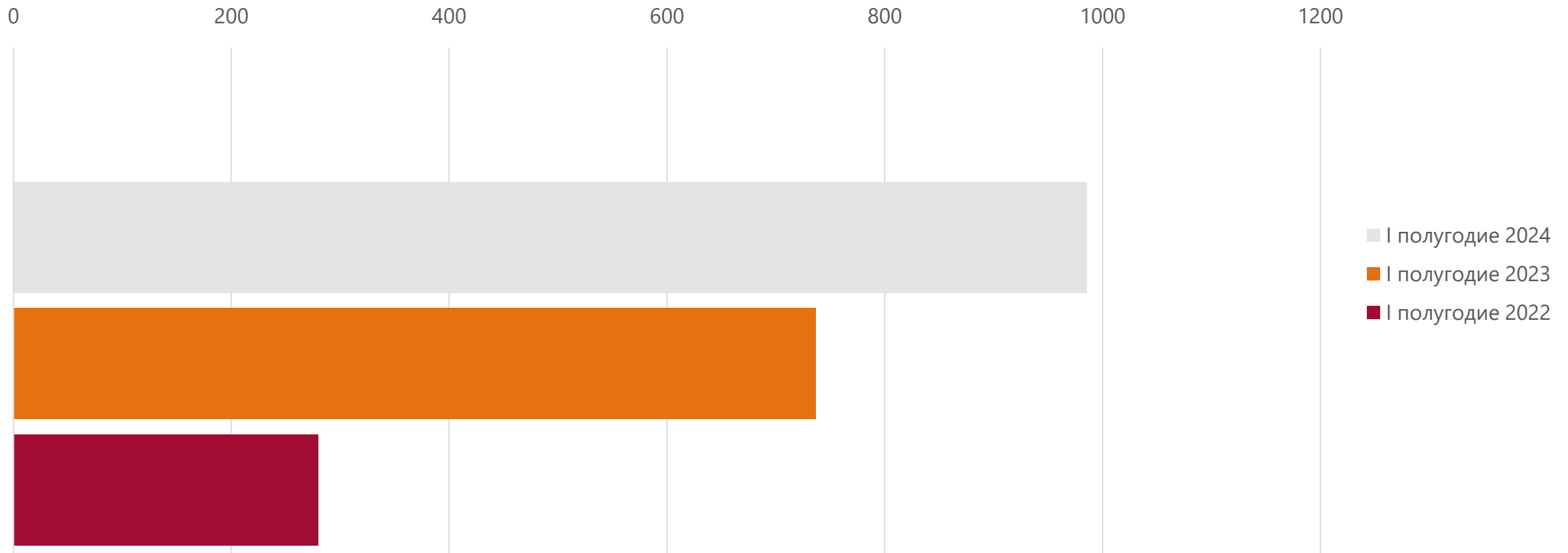
Количество утечек информации в России

2024



В России «утекло» почти миллиард записей персональных данных

2024

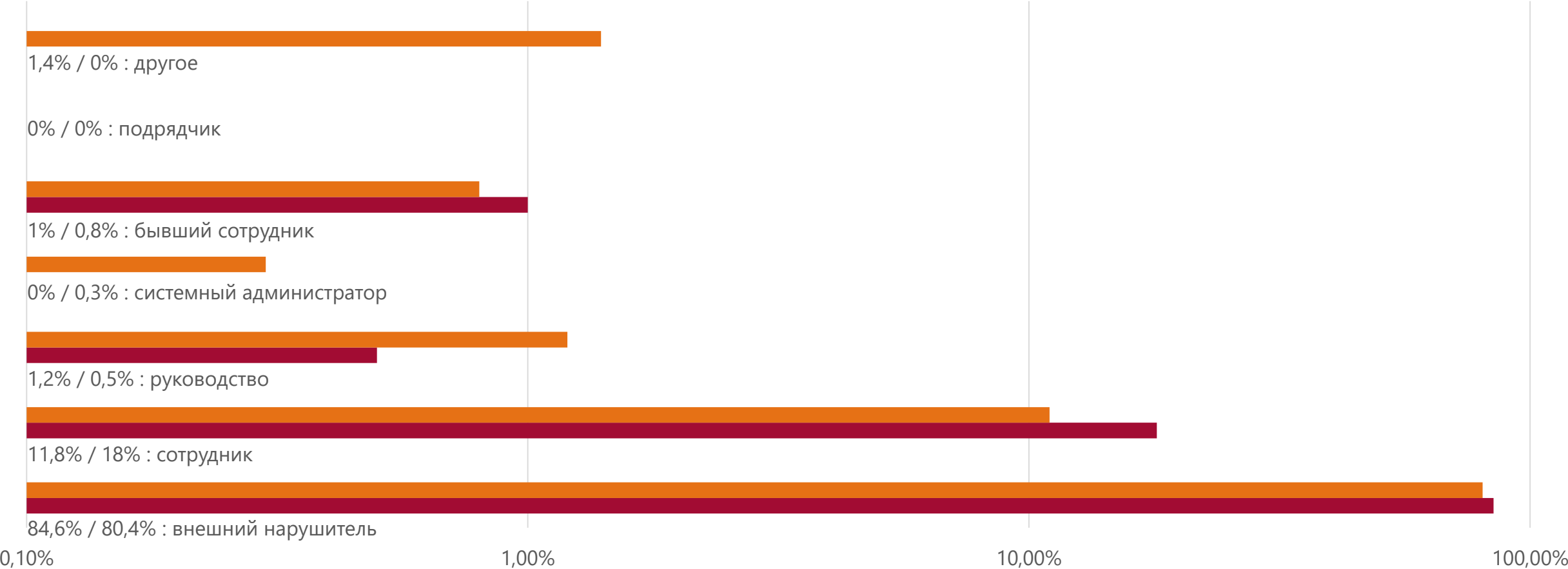


Количество утекших записей ПДн (в миллионах): Россия, I полугодие 2022 г., I полугодие 2023 г., I полугодие 2024 г

Виновники утечек информации

2024

Виновники утечек информации: Россия, I полугодие 2024 г. – I полугодие 2024 г.



Последствия утечек ПДн в 2025 году: от административного штрафа до лишения свободы

2024

Законопроект № 502104-8 (ст. 13.11. КоАП РФ)		Штраф	
Совершённое действие		Сотрудник	Компания
▪ Неуведомление Роскомнадзора об утечке ПДн		До 800 тыс.	До 3 млн.
▪ Бездействие оператора, повлекшие утечку ПДн		До 4 млн.	До 500 млн.
▪ Утечка специальных ПДн		От 1,5 до 5 млн	От 10 до 500 млн

Законопроект № 502113-8 (ст. 272.1. УК РФ)	Штраф	Лишение свободы
▪ Уголовная ответственность за незаконное использование персональных данных:	До 3 млн	До 10 лет

**ОБУЧЕНИЕ РАБОТНИКОВ ПРАВИЛАМ
ОБРАБОТКИ И ЗАЩИТЫ ПДН **ПРЕДПИСАНО**
ЗАКОНОМ**

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

• **Назначение** оператором, являющимся юридическим лицом, **ответственного** за организацию обработки персональных данных;

• **Применение правовых, организационных и технических мер** по обеспечению безопасности персональных данных;

• **Осуществление внутреннего контроля** и (или) аудита соответствия обработки персональных данных законодательству, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

• **Ознакомление работников** оператора, непосредственно **осуществляющих обработку персональных данных**, с положениями законодательства 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, **обучение** указанных **работников**.



Постановление Правительства РФ от 21.03.2012 N 211

2024

«Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

Операторы осуществляют ознакомление служащих с положениями законодательства с требованиями к защите персональных данных, локальными актами и организуют обучение указанных служащих.



«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Лица, осуществляющие обработку персональных данных должны быть проинформированы об особенностях и правилах осуществления такой обработки.

- Обеспечение защиты информации должно осуществляться оператором и включать **информирование и обучение персонала.**

- **Периодичность** проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала **не реже 1 раза в два года.**

18.6. В ходе **информирования и обучения персонала** информационной системы осуществляются:

- **Информирование персонала** информационной системы о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы;
- **Доведение до персонала информационной** системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;
- **Обучение персонала** информационной системы правилам эксплуатации отдельных средств защиты информации;
- **Проведение практических занятий и тренировок** с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;
- Контроль **осведомленности персонала** информационной системы об угрозах безопасности информации и **уровня знаний персонала** по вопросам обеспечения защиты информации

Приказ ФСТЭК России от 25.12.2017 N 239

2024

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»

13. Обеспечение безопасности в ходе эксплуатации **значимого объекта осуществляется субъектом КИИ** в соответствии с эксплуатационной документацией и организационно-распорядительными документами по безопасности значимого объекта и **должно включать реализацию следующих мероприятий:** планирование мероприятий, анализ угроз безопасности, реагирование на компьютерные инциденты, обеспечение действий в нештатных ситуациях, **информирование и обучение персонала значимого объекта.**

13.7. В ходе информирования и обучения персонала значимого объекта осуществляются:

- **Информирование персонала** об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта
- **Доведение до персонала требований** по обеспечению безопасности значимых объектов, а также **положений** организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся
- **Обучение персонала** правилам эксплуатации отдельных средств защиты информации, включая **проведение практических занятий** с персоналом
- **Контроль осведомленности персонала** об угрозах безопасности информации **и уровня знаний персонала** по вопросам обеспечения безопасности КИИ

**КОМПЕТЕНЦИИ СОТРУДНИКОВ
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПДН:
ИЗМЕНЕНИЯ В ЗАКОНОДАТЕЛЬСТВЕ И
ПЕРСПЕКТИВЫ РАЗВИТИЯ**

Изменения в Приказе ФСТЭК России от 21.12.2017 N 235

2024

«Об утверждении требований к созданию систем безопасности объектов КИИ»

12. Работники структурного подразделения по безопасности, специалисты по безопасности должны соответствовать следующим требованиям:

- **Наличие у руководителя** структурного подразделения **по безопасности** высшего профессионального **образования** по направлению подготовки (специальности) **в области информационной безопасности** или иного высшего профессионального образования и документа, подтверждающего прохождение **обучения** по программе профессиональной **переподготовки** по направлению **«Информационная безопасность»**, наличие стажа работы в сфере информационной безопасности не менее 3 лет (в ред.Приказа ФСТЭК России от **20.04.2023** №69)

- **Наличие у штатных работников** структурного подразделения **по безопасности**, штатных специалистов по безопасности профессионального образования по направлению подготовки (специальности) **в области информационной безопасности** или иного высшего профессионального образования **с прохождением обучения по программе повышения квалификации по направлению «Информационная безопасность»** (в ред.Приказа ФСТЭК России от **20.04.2023** №69)

- **Прохождение не реже одного раза в 3 года обучения по программам повышения квалификации по направлению «Информационная безопасность».** (в ред.Приказа ФСТЭК России от **20.04.2023** №69).



Изменения в Приказе ФСТЭК России от 21.12.2017 N 235

2024

«Об утверждении требований к созданию систем безопасности объектов КИИ»

25. Организационно-распорядительные документы по безопасности значимых объектов должны определять:

- 01** Цели и задачи обеспечения безопасности значимых объектов КИИ, основные угрозы безопасности информации и категории нарушителей, основные **организационные** и технические мероприятия по обеспечению безопасности значимых объектов КИИ, проводимые субъектом КИИ, состав и структуру системы безопасности и функции ее участников, порядок применения, формы оценки соответствия значимых объектов КИИ и средств защиты информации требованиям по безопасности
- 02** **Планы мероприятий по обеспечению безопасности** значимых объектов КИИ, модели угроз безопасности информации в отношении значимых объектов КИИ, порядок реализации отдельных мер по обеспечению безопасности значимых объектов КИИ, порядок проведения испытаний или приемки средств защиты информации, порядок реагирования на компьютерные инциденты, **порядок информирования и обучения работников**, порядок взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов КИИ, порядок взаимодействия субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- 03** **Правила безопасной работы** работников субъекта КИИ на значимых объектах КИИ, **действия работников** субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.

Изменения в Приказе ФСТЭК России от 21.12.2017 N 235

2024

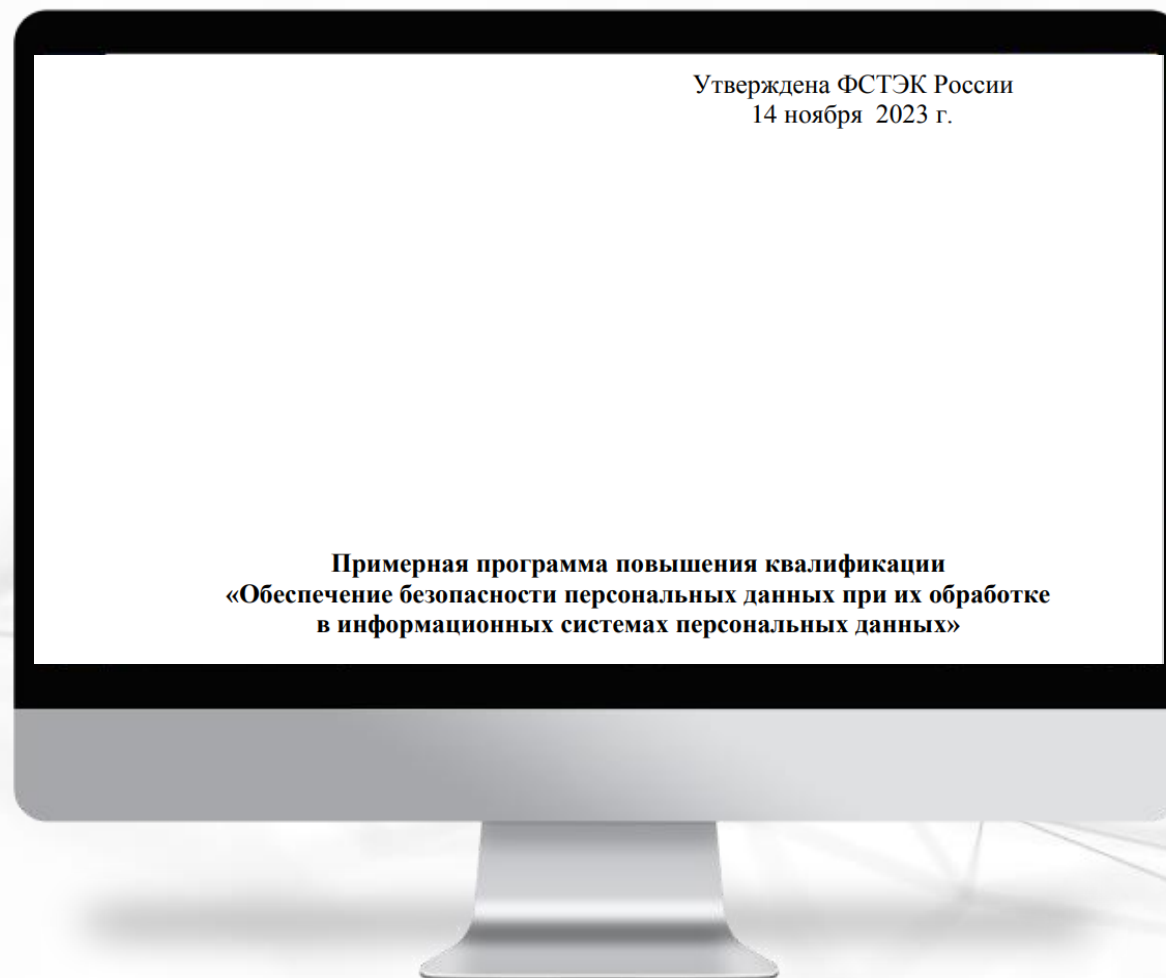
«Об утверждении требований к созданию систем безопасности объектов КИИ»

27. Организационно-распорядительные документы по безопасности значимых объектов должны быть доведены до руководства субъекта КИИ, ответственного лица, подразделения по безопасности, специалистов по безопасности, а также до **иных подразделений (работников)**, участвующих в обеспечении безопасности значимых объектов КИИ, в части, их касающейся (в ред. Приказа ФСТЭК России от 20.04.2023 №69).



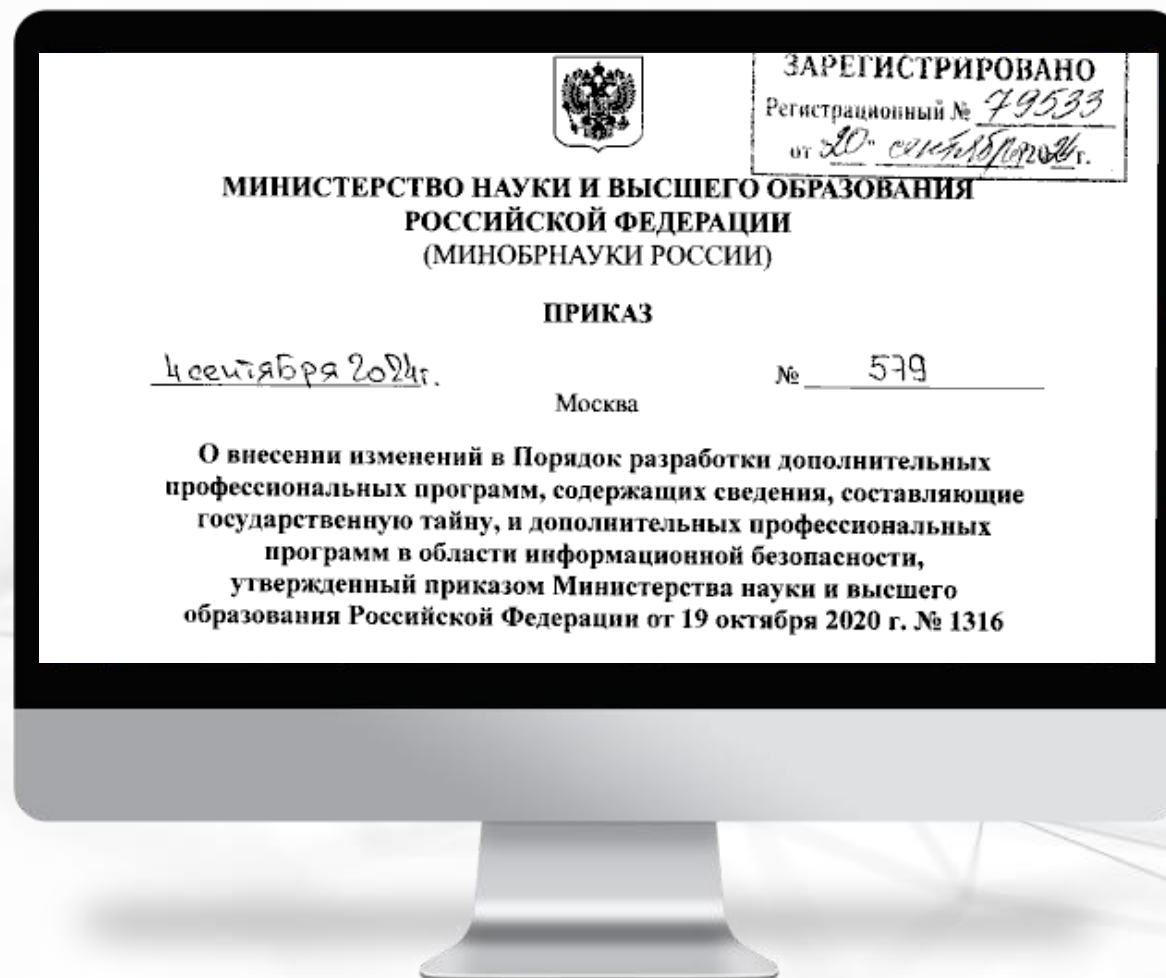
ФСТЭК России обновил программу повышения квалификации по ПДн

2024



Приказ Министерства науки и высшего образования Российской Федерации от 04.09.2024 № 579

2024



Новые профстандарты по информационной безопасности

2024

Зарегистрировано в Минюсте России 14 октября 2022 г. N 70543

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
от 14 сентября 2022 г. N 525н
ОБ УТВЕРЖДЕНИИ ПРОФЕССИОНАЛЬНОГО СТАНДАРТА
"СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В
АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ"

В соответствии с [пунктом 16](#) Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. N 23 (Собрание законодательства Российской Федерации, 2013, N 4, ст. 293; 2014, N 39, ст. 5266), приказываю:

1. Утвердить прилагаемый профессиональный стандарт "Специалист по защите информации в автоматизированных системах".
2. Признать утратившим силу приказ Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857).
3. Установить, что настоящий приказ вступает в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Министр
А.О. КОТЯКОВ

Зарегистрировано в Минюсте России 22 декабря 2022 г. N 71784

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
от 28 ноября 2022 г. N 739н
ОБ УТВЕРЖДЕНИИ ПРОФЕССИОНАЛЬНОГО СТАНДАРТА
"СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ"

В соответствии с [пунктом 16](#) Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. N 23 (Собрание законодательства Российской Федерации, 2013, N 4, ст. 293; 2014, N 39, ст. 5266), приказываю:

1. Утвердить прилагаемый профессиональный стандарт "Специалист по информационной безопасности в кредитно-финансовой сфере".
2. Установить, что настоящий приказ вступает в силу с 1 сентября 2023 г. и действует до 1 сентября 2029 г.

Министр
А.О. КОТЯКОВ

Новые профстандарты по информационной безопасности

2024



Изменения 152-ФЗ о государственном контроле и надзоре за выполнением мер по обеспечению безопасности ПДн

2024

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

9. Решением Правительства РФ с **учетом значимости и содержания обрабатываемых персональных данных ФСБ России** может быть **наделена полномочиями по контролю за выполнением организационных** и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, **при их обработке в ИСПДн**, эксплуатируемых при осуществлении определенных видов деятельности и **не являющихся государственными** информационными системами персональных данных. Решением Правительства РФ с учетом значимости и содержания обрабатываемых персональных данных **ФСТЭК России** также может быть **наделена указанными полномочиями** без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных **(часть 9 в ред. ФЗ от 08.08.2024 №233-ФЗ).**

8. **Контроль и надзор за выполнением организационных** и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в государственных ИСПДн, а также в эксплуатируемых в государственных органах РФ **иных ИСПДн** осуществляется ФСБ и ФСТЭК России **(часть 8 в ред. ФЗ от 08.08.2024 №233-ФЗ).**

ОБРАЗОВАТЕЛЬНЫЕ РЕШЕНИЯ

Академия Softline

Партнер для кастомизированного проектного обучения. Мы помогаем нашим заказчикам развивать бизнес и трансформироваться через подготовку квалифицированных кадров.

Проводим масштабные образовательные проекты, профессиональную переподготовку, программы повышения квалификации, курсы по самым востребованным направлениям. Разрабатываем образовательный контент под потребности заказчика.

29+

лет опыта на рынке
дополнительного
профессионального
образования

1 место

в ТОП-10 самых быстрорастущих
компаний в сегменте ДПО по итогам
2023 года

5 млн. +

выпускников

15 000+

корпоративных и государственных
заказчиков

1 место

в рейтинге образовательных
организаций AstraLinux

400+

экспертов в разработке
и поставке обучения

5 место

в ТОП-10 самых динамично растущих
edtech компаний по итогам 2023 года

Направления обучения

2024



Авторизованное обучение,
сертификация



Информационная
безопасность



Цифровые профессии



Лаборатория цифровой
трансформации



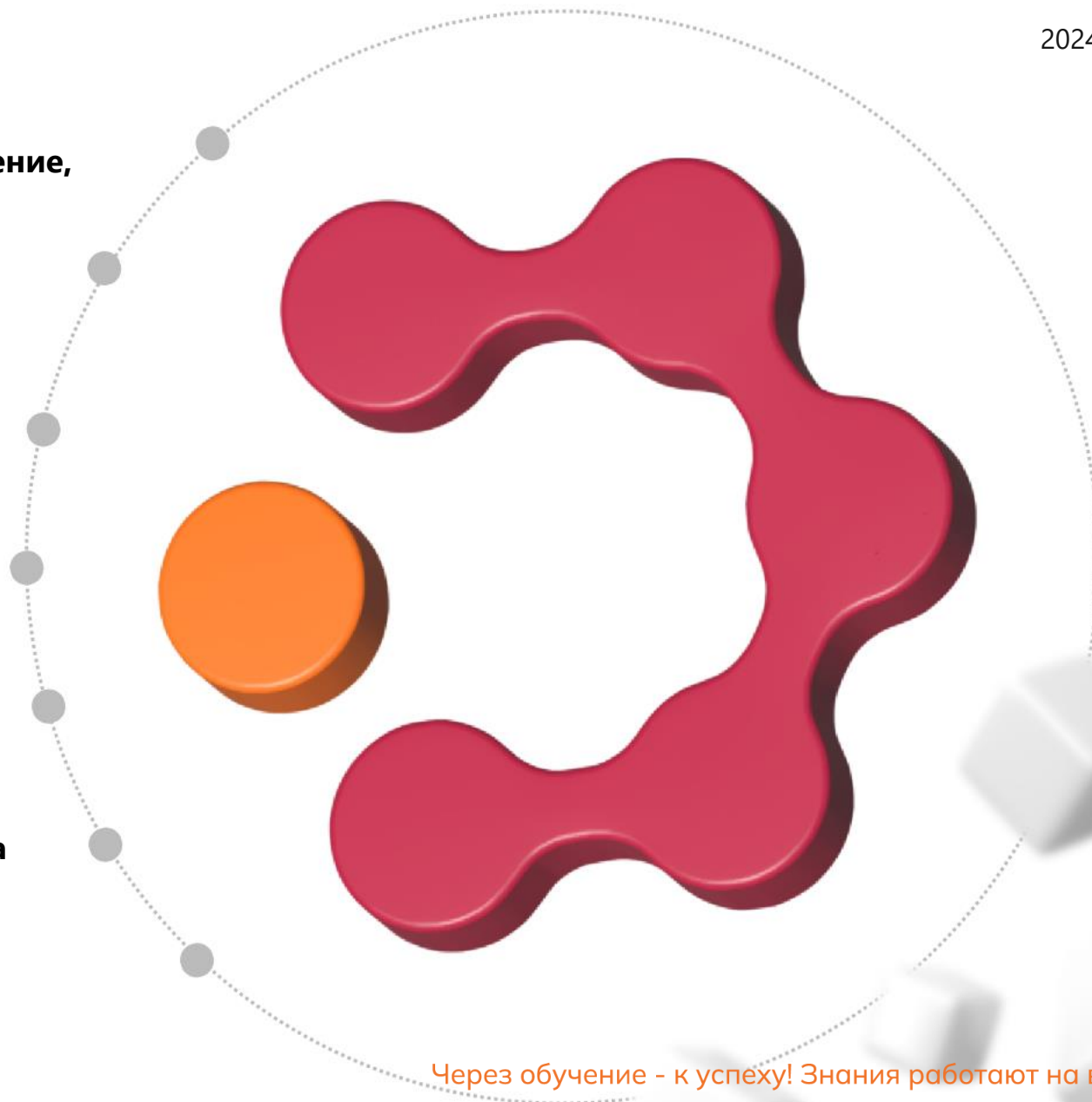
EdTech решения



Разработка
образовательного контента



Подбор команд в штат
через обучение



Возможности обучения

2024

Программы повышения квалификации, проф.переподготовки. Для специалистов и руководителей по ИБ.

Мультиформатность – очно на территории заказчика или дистанционно онлайн.

85+

Курсов в портфеле по защите информации



Защита персональных данных в организации



Защита персональных данных в специализированных отраслях: медицинские учреждения, госсектор.



Готовые электронные курсы для широкой аудитории



Мастер-классы с конкретными приемами защиты от социальной инженерии

Нам доверяют



УЭМЗ
РОСАТОМ



ЯРМИАЦ
Якутский республиканский медицинский
информационно-аналитический центр



СБЕР



**ГАЗПРОМ
ТРАНС**



таграс
все грани сервиса



ТЭК ИНФОРМ
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ



X5RETAILGROUP

росбанк



Сеченовский
Университет
наук о жизни



ВТБ



1890
КНИТУ

Программы обучения, согласованные с регуляторами

2024

-  Программы согласованы с ФСТЭК, ФСБ России и другими регуляторами
-  Программы соответствуют текущим изменениям в законодательстве
-  Программы содержат комплексные знания и около 50% практических занятий
-  Контроль представителей органов за учебной программой

Программы по защите персональных данных

ТЗКИ011

Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие гостайну.

 112 ак.часов.  Удостоверение по повышению квалификации

Слушатель получит комплексные знания и навыки в технической защите информации (ТЗИ)

ТЗКИ001

Комплексная защита персональных данных.

 72 ак.часов.  Удостоверение по повышению квалификации

Слушатель получит комплексные знания и навыки по обеспечению обработке и защиты персональных данных в соответствии с требованиями законодательства

Программы обучения, согласованные с регуляторами

2024

Специализированные программы

ТЗКИ013

Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа

🕒 112 ак.часов. 🎓 Удостоверение по повышению квалификации + сертификат от «Код Безопасности».

Флагманские программы

КИИ187

Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

🕒 108 ак.часов. 🎓 Удостоверение по повышению квалификации

ТЗКИ512

Информационная безопасность. Техническая защита конфиденциальной информации.

🕒 512 ак.часов. 🎓 Диплом установленного образца

КИИ502

Информационная безопасность. Безопасность значимых критической информационной инфраструктуры

🕒 502 ак.часов. 🎓 Диплом установленного образца

ИБКИИ512

Информационная безопасность. Обеспечение защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

🕒 512 ак.часов. 🎓 Диплом установленного образца

Найм персонала в штат через обучение

Школа ИБ-кадры

О решении

Решение для ИТ, ИБ-рекрутинга «Школа ИТ и ИБ-кадры» включает в себя организацию стажёрских программ под ключ для корпоративных клиентов.

Мы обучаем команды под любые технологические стеки заказчика.



Помогаем в адаптации специалистов уровня Junior и Middle

Что получает клиент

Обученную, замотивированную команду, объединенную общими целями и корпоративной культурой.

82%

Партнеров запускают школу 3-й и более раз

30%

Сокращается отток кандидатов

30%

В среднем повышается лояльность к HR-бренду

90%

Стажёров довольны результатами участия

75%

Практико-ориентированных занятий

74%

Конверсия стажёров в штат

Стажерская программа **Школа ИБ**

2024

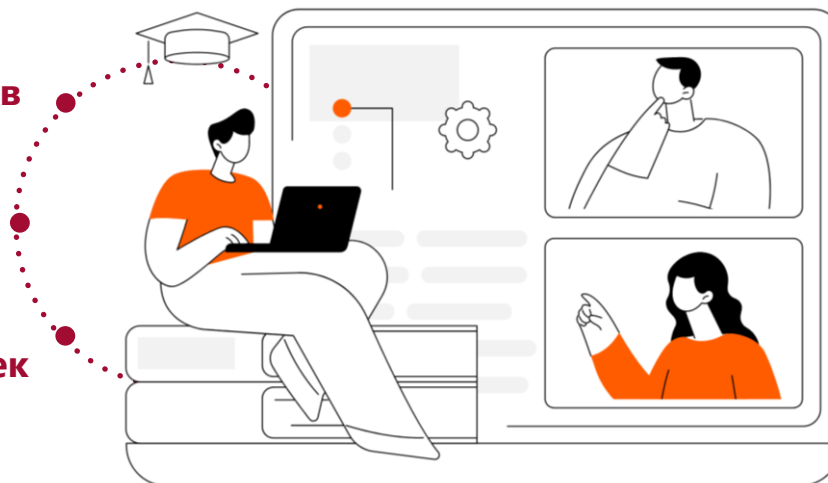
Кейс Банк ВТБ

Программа сочетала в себе интенсивное обучение в области **обеспечения информационной безопасности, а также изучение технологий защиты банковских систем** с применением их на практике.

**Очное обучение
в Москве для выпускников
московских ВУЗов**

**Разработали индивидуальный
план обучения**

**Отобрали 4 группы
студентов по 15 человек**



**Положительность -
3 месяца**

**Администраторы ИБ,
пентестеры**

**По итогам тестирования
отобрали лучших студентов в
штат банка**

Подробнее о проекте:

<https://vtbcareer.com/internship/it-school/>

<https://changellenge.com/>



Разработка курса от 2-х недель



Вариативность форматов курса и видов
контента



Живое общение с преподавателем,
который дает объективную оценку

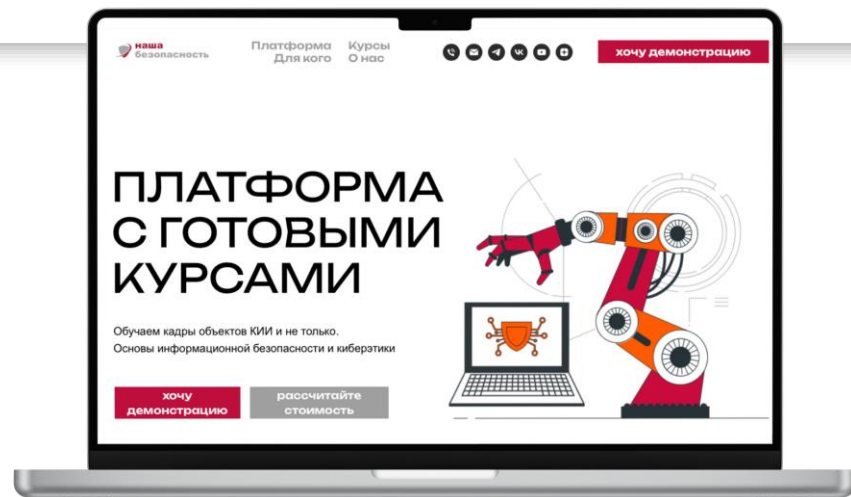


Ресурсы 400+ экспертов, кандидатов наук

Повышение осведомленности в ИБ



Платформа «Наша безопасность» — комплексная система обеспечения осведомленности персонала в Информационной безопасности



Какие задачи решает сервис:



Обучение и тренировка персонала



Навыки распознавания угроз



Снижение рисков ИБ



Оценка компетенций



Ключевые преимущества:

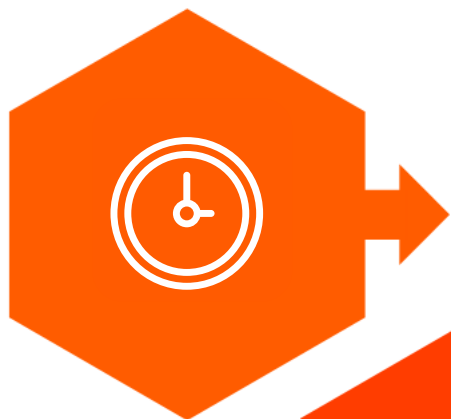
- ▶ Быстрое решение «под ключ», оформленное в фирменном стиле заказчика
- ▶ Автоматизация обучения
- ▶ Удобная установка на сервер или подписка на облачный сервис
- ▶ Удобное управление образовательным процессом
- ▶ Статистика и отчёты
- ▶ 6 бесплатных курсов в базовом пакете
- ▶ Бесплатная техническая поддержка на 3 мес.
- ▶ Возможность развития платформы и контента под заказчика

Результат. Наша безопасность

2024

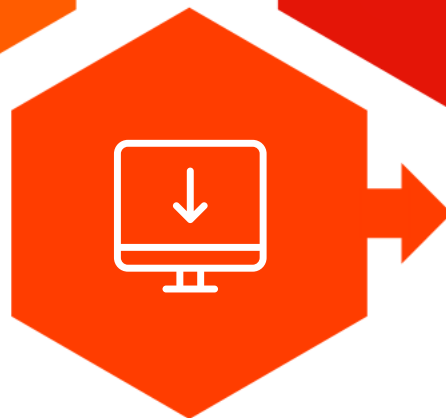
01

Сервис обучения,
доступный
в режиме 24x7



02

Пакет интерактивных
курсов по повышению
осведомленности



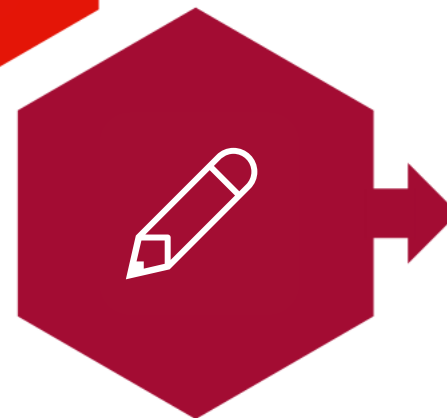
03

Централизованная база
результатов обучения



04

Возможность проходить
обучение большому числу
персонала, в любое удобное
время, единое качество
обучения, единые критерии
оценки



Летний детский лагерь «Наша безопасность»

2024

Для сотрудников ГК Softline

Бесплатно

Онлайн

80+

участников лагеря

5 недель

обучения и общения

30+

полезных чек-листов,
инструкций, статей
и материалов по
цифровой гигиене



Общение, квесты,
викторины в канале
лагеря с вожатыми



Вебинары
и мастер-классы
с экспертами



6 курсов
онлайн



Сертификаты
и призы



академия **softline** 

Через обучение - к успеху! Знания работают на вас

Программы взаимодействия с ВУЗами

Академия Softline - спонсор межвузовских штабных киберучений «IrkCyberDef» на базе Иркутского Политеха (национального исследовательского университета)

- отработка профессиональных и «гибких» навыков
- решение реальных кейсов
- обратная связь от действующих экспертов по защите информации
- взаимодействие с органами власти
- стажировка в компании Softline с последующим заключением трудовых договоров



Спасибо за внимание!



Academy@academyit.ru
Academyit.ru



Тел: +7 (495) 150-96-00



Через обучение - к успеху!
Знания работают на вас