



КУЗБАССКАЯ
ТОРГОВО-ПРОМЫШЛЕННАЯ
ПАЛАТА

«Кибербезопасность и защита данных»

Комитет по безопасности предпринимательской деятельности

Кожевников Вадим Витальевич

- Член Комитета по безопасности предпринимательской деятельности Кузбасской ТПП;
- Юрист – 25 лет стажа;
- Эксперт и автор вебинаров по защите персональных данных;
- Эксперт в области обеспечения защиты персональных данных в медицинских организациях



ПРОГРАММА

Киберугрозы: что актуально для бизнеса

Основные виды угроз и уязвимостей

Персональные данные и требования по их защите

Практические решения по защите персональных данных

Наиболее частые ошибки компаний



Киберугрозы

Киберугроза — это реальные риски для любой компании, которые могут привести к финансовым потерям, утечек конфиденциальной информации и потере репутации.

Кибератака может нанести вред компьютерным системам, сетям или данным организации.

Киберугрозы могут быть связаны с разным вредоносным ПО (вирусы, шпионское ПО, программы-вымогатели), фишинговыми атаками, DDoS-атаками и другими методами, используемыми для проникновения и повреждения информационной инфраструктуры.



Основные тенденции киберугроз

- I. Рост числа целевых атак на компании малого и среднего бизнеса, а не только на крупные корпорации;
- II. Использование искусственного интеллекта злоумышленниками для автоматизации атак и подбора уязвимостей;
- III. Увеличение случаев фишинга и социальной инженерии, направленных непосредственно на сотрудников;
- IV. Распространение вымогательских программ, когда доступ к данным блокируется до уплаты выкупа;
- V. Активизация атак на цепочки поставок и подрядчиков, через которых злоумышленники получают доступ к крупным объектам.



Реальные примеры атак

- I. В результате атак с использованием шифровальщиков крупные мировые корпорации простаивали по несколько дней, теряя миллионы долларов;
- II. Попытки взлома бухгалтерских и казначейских систем компаний, когда мошенники перенаправляли платежи на свои счета;
- III. Случаи компрометации корпоративной почты, которая приводит к утечке коммерческой тайны и срывам
- IV. Атаки на подрядчиков привели к остановке работы целых цепочек поставок

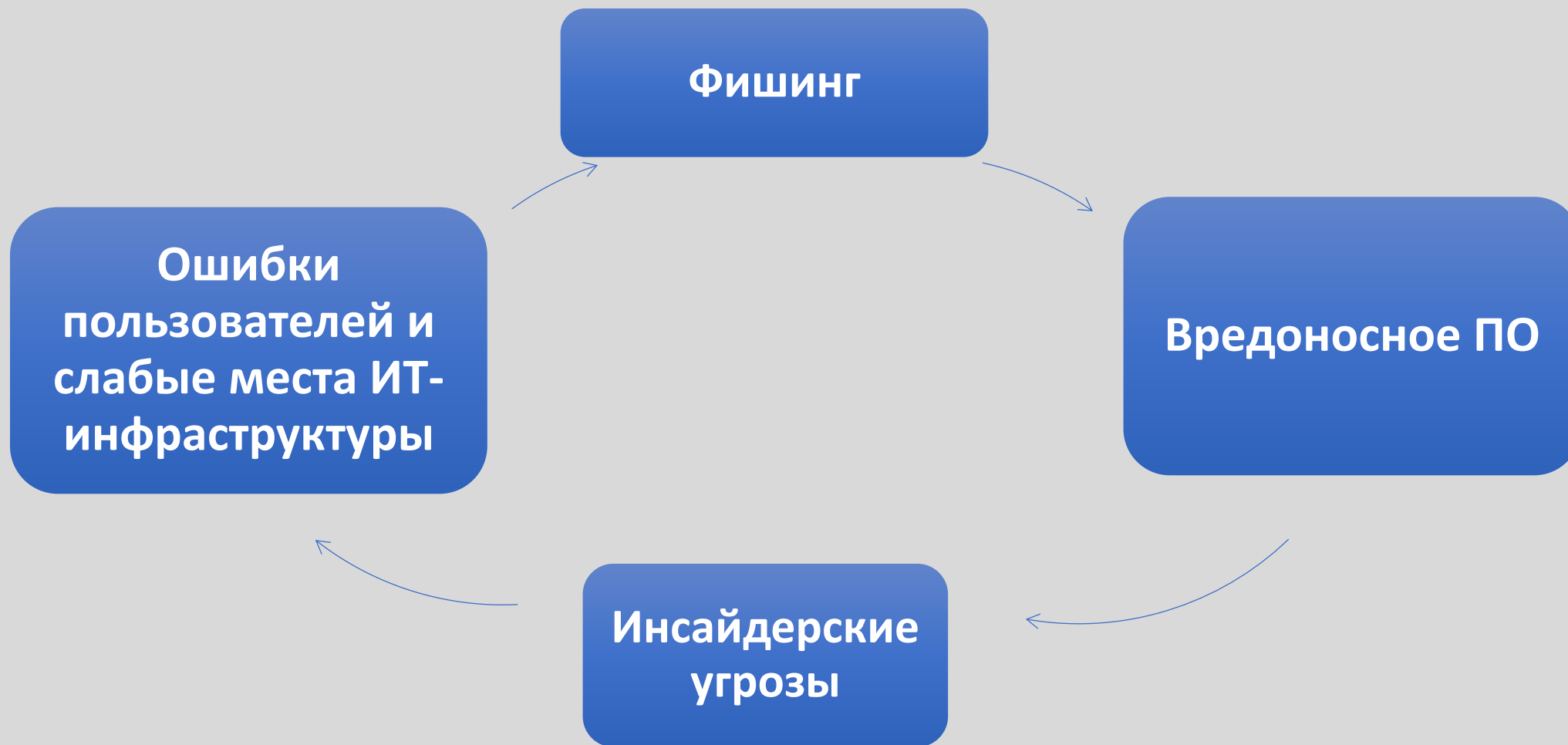


Последствия нарушений кибербезопасности

- Прямые финансовые убытки — от выплаты вымогателям до простоя производства и срыва контрактов;
- Утечка конфиденциальной информации, которая часто имеет стоимость выше самих денег на счетах;
- Репутационные потери: падение доверия клиентов и партнеров может стать фатальным;
- Рост регуляторных рисков и штрафов за нарушение законодательства о защите данных;
- Кадровые последствия, когда сотрудники теряют уверенность в надежности компании.



Основные виды угроз и уязвимостей



Фишинг

Фишинг -это вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователей, таких как пароли, банковские реквизиты и другая важная информация. Злоумышленники посылают поддельные электронные письма или сообщения, имитирующие официальные уведомления от банков, провайдеров или других организаций, с просьбой срочно передать или обновить личные данные. Эти сообщения часто содержат угрозы блокировки счетов или других негативных последствий, если пользователь не выполнит требования.

Фишинг остается одним из самых распространенных и эффективных методов атак. Злоумышленники маскируются под доверенных отправителей, чтобы обманом получить конфиденциальные данные сотрудников.

Современный фишинг все чаще использует искусственный интеллект для повышения качества текста и персонализации сообщений, что затрудняет распознавание угрозы. Это одна из главных причин, почему обучение сотрудников кибергигиене является критически важным.



Примеры кибератак

- I. Фальшивая доставка цветов, подарков, пиццы и т.д. Просьба оплатить комиссию за доставку.
- II. Замена домофона, сотовые операторы, ЦБ/служба безопасности банков
- III. По данным Центра кибербезопасности, 37% инцидентов были связаны с майнерами криптовалют, а загрузка пользователями вредоносных программ из непроверенных источников стала самым распространённым вектором компрометации.
- IV. Кибермошенники активно вовлекают подростков в преступления, связанные с дропперством, порчей имущества, вербовкой.



Вредоносное ПО

Вредоносное ПО- вредоносное программное обеспечение

Вирусы — *самостоятельно распространяющиеся программы, повреждающие файлы и системы;*

Трояны — *маскирующиеся под полезное ПО для скрытого внедрения и захвата контроля;*

- **Шифровальщики (ransomware)** — *блокируют данные и требуют выкуп за разблокировку;*

Шпионское ПО — *следит за действиями пользователя и крадет информацию;*

Пути заражения — *через вложения в письмах, уязвимости в ПО, зараженные съемные носители или уязвимости сети.*



Инсайдерские угрозы

Инсайдерские угрозы исходит изнутри организации, когда сотрудники или партнеры компании сознательно или по неосторожности становятся источником утечек или нарушений безопасности.

Это могут быть как преднамеренные действия (например, передача данных конкурентам), так и случайные ошибки или несоблюдение установленных правил. Часто именно человеческий фактор становится слабым звеном в ИТ-системе.

Инсайдерские угрозы особенно сложны для обнаружения и предотвращения, так как нарушители имеют законный доступ к системам.



Ошибки пользователей и слабые места ИТ-инфраструктуры

- I. Человеческий фактор — ключевое слабое место в ИТ-безопасности. Частые ошибки — использование простых паролей, клики по подозрительным ссылкам, игнорирование обновлений и рекомендаций службы безопасности. Отсутствие регулярного обучения сотрудников по кибергигиене увеличивает шансы успешной атаки.

Комплексный подход к безопасности должен учитывать технические и организационные меры: регулярное обучение сотрудников, своевременное обновление систем, внедрение средств обнаружения угроз и построение культуры ответственности в компании. Только так можно снизить вероятность успешных кибератак и защитить бизнес от финансовых и репутационных потерь.

- I. Использование простых паролей, пренебрежение обновлениями и неправильные действия при подозрительных сообщениях, значительно повышают риски. Кроме того, уязвимости в ИТ-инфраструктуре — устаревшее ПО, отсутствие сегментации сети, недостаточный уровень контроля доступа — создают возможности для успешных атак.



Основные правила защиты

- **Не сообщайте личные данные:** Никогда не передавайте незнакомцам свои пароли, коды из SMS, данные банковских карт или паспорта.
- **Будьте скептически к предложениям:** Относитесь с осторожностью к слишком заманчивым предложениям и обещаниям легких денег.
- **Проверяйте отправителя:** Не переходите по подозрительным ссылкам из SMS, писем или сообщений от неизвестных отправителей.
- **Проверяйте ссылки и сайты:** Убедитесь, что сайт настоящий, внимательно изучив адрес в адресной строке.
- **Не устанавливайте неизвестные программы:** Не загружайте приложения из непроверенных источников и не следуйте инструкциям по установке ПО от незнакомцев, особенно через ссылки.



Как защититься от основных угроз

- Регулярные тренинги для сотрудников по распознаванию угроз и действиям при подозрениях;
- Внедрение современных антивирусных систем, систем обнаружения вторжений, многофакторной аутентификации;
- Постоянный мониторинг инфраструктуры и тестирование на уязвимости;
- Разработка и отработка плана реагирования на инциденты, включая резервное копирование



Персональные данные и требования по их защите

Основным нормативным актом является Федеральный закон № 152-ФЗ «О персональных данных», который регулирует сбор, хранение, обработку и защиту личной информации граждан.

В 2025-2026 годах были приняты важные поправки и изменения, направленные на ужесточение контроля и повышение ответственности за нарушение требований:

- введена единая форма согласия на обработку персональных данных, обязательная для всех операторов данных;
- усилены требования к локализации данных — с 1 июля 2025 года запрещено хранение баз персональных данных за рубежом, так называемая «трансграничная передача данных»;
- операторы обязаны передавать обезличенные массивы данных по запросу регуляторов;
- повышены штрафы за несоблюдение требований закона — для юридических лиц они могут достигать до 20 000 000 рублей!;
- введена уголовная ответственность за незаконное использование, передачу и хранение персональных данных, вплоть до лишения свободы сроком до 6 лет в особо тяжких случаях.



Ответственность за нарушение

**За нарушения законодательства установлены три вида ответственности:
административная, гражданско-правовая и уголовная**

- 1) Административные штрафы применяются за неправильную обработку данных, нарушение требований по локализации и информационной безопасности, несвоевременное уведомление об инцидентах.
- 2) Гражданско-правовая ответственность наступает, если нарушитель причинил убытки или моральный вред субъектам данных.
- 3) Уголовная ответственность предусмотрена для серьёзных правонарушений, таких как незаконный сбор и передача личных данных, с наказаниями вплоть до тюремного заключения.



Примеры утечки персональных данных

- За 2025 год и первое полугодие 2026 года в России зафиксировано 326 утечек, в результате которых было скомпрометировано 1,175 млрд строк с данными пользователей
- В феврале 2025 года хакерская группировка «Silent Crow» заявила о взломе ИТ-инфраструктуры. Были похищены данные, включая ФИО, телефоны, email, паспортные данные и адреса. Впоследствии в открытый доступ выложили более 10 млн записей
- МФО «ГринМани»: В октябре 2026 года из-за ошибки в конфигурации базы данных в открытом доступе оказались кредитные истории более чем миллиона россиян. В слитых документах содержались паспортные данные, телефоны, адреса и сведения о кредитах.
- Авиакомпания «Аэрофлот»: В июле 2025 года хакеры из групп «Киберпартизаны» и Silent Crow заявили о масштабном взломе, в результате которого могли быть украдены 20 Тб данных. Позже часть информации, включая данные о перелетах руководства, была опубликована
- Фитнес-клуб DDX: В августе 2026 года произошла утечка, в результате которой в Сеть попали контакты и персональные данные сотен звезд шоу-бизнеса и спорта

Персональные данные — это ценный актив, и их защита требует комплексного подхода, включая как технические меры, так и юридическую ответственность. Соблюдение законодательства в этом вопросе защищает бизнес от серьёзных финансовых и репутационных рисков.



Рекомендации по организации защиты персональных данных

1. Анализ и классификация данных

- Выявить, какие персональные данные обрабатываются в компании, и классифицировать их по степени чувствительности.
- Определить цели и легальность обработки этих данных согласно требованиям законодательства.

2. Разработка и внедрение политики безопасности

- Создать внутренние документы по защите персональных данных: политики, инструкции, регламенты.
- Назначить ответственных за защиту данных и ИТ-безопасность.
- Обеспечить регулярное обучение сотрудников по вопросам конфиденциальности и безопасности.



Рекомендации по организации защиты персональных данных

3. Технические меры защиты

- Использовать шифрование данных в состоянии покоя и при передаче.
- Внедрить системы контроля доступа с ролями и многофакторной аутентификацией.
- Регулярно обновлять программное обеспечение и применять патчи для устранения уязвимостей.
- Использовать антивирусные и антифишинговые решения, системы обнаружения вторжений (IDS/IPS).
- Обеспечить регулярное резервное копирование и хранение копий в защищенном месте.



Рекомендации по организации защиты персональных данных

4. Организационные меры

- Ограничить доступ к персональным данным только тем сотрудникам, для которых это необходимо.
- Проводить аудит и мониторинг доступа и действий с данными.
- Внедрить процессы уведомления о киберинцидентах и их расследования.
- Планировать и отрабатывать действия по реагированию при утечках или нарушениях безопасности.

5. Соответствие законодательству и контроль

- Следить за изменениями в законодательстве и своевременно адаптировать внутренние процессы.
- Проводить регулярные внутренние и внешние аудиты защиты данных.
- Документировать все процессы обработки и меры защиты.



Кейсы и наиболее частые ошибки компаний

Аудит безопасности — это системный и комплексный процесс проверки и оценки текущего состояния системы безопасности (чаще информационной), с целью выявления уязвимостей, угроз и слабых мест в защите, а также оценки рисков. Он включает анализ бизнес-процессов, технических средств и процедур безопасности, с последующей выдачей рекомендаций по улучшению системы защиты.

Выявление критических точек

- Определение этапов или мест с максимальным риском.
- Контроль и мониторинг этих точек для предотвращения угроз.
- Пример: в пищевой промышленности это этапы, где возможна порча или загрязнение продукции.
- В контексте информационной безопасности это могут быть слабые места в защите систем, доступы, каналы утечки и пр.



Ошибки в защите резервных копий

- ✓ **Недостаточная защита доступа.** Часто права на управление и доступ к резервным копиям имеют слишком широкие группы сотрудников или специалисты с низкой квалификацией, что повышает риск случайного или преднамеренного нарушения целостности резервных данных. Рекомендуется строго контролировать и ограничивать доступ через аутентификацию, авторизацию и разделение прав ответственности.
- ✓ **Отсутствие шифрования копий и каналов передачи.** Если резервные данные и каналы, по которым они передаются, не защищены паролями и не шифруются, это создает возможность перехвата, чтения или изменения данных злоумышленниками.
- ✓ **Хранение резервных копий в том же месте, что и оригинальные данные,** делает копии уязвимыми при физическом повреждении, пожаре, кибератаках, например шифровальщиками.
- ✓ **Попадание в резервные копии уже зараженных вредоносным ПО файлов,** что приводит к восстановлению зараженной системы.
- ✓ **Отсутствие регулярного тестирования восстановления** приводит к ситуации, когда при необходимости оказывается, что резервные копии повреждены или неподходящего формата.
- ✓ **Уязвимость резервных копий** перед атаками шифровальщиков и удалением данных через скомпрометированные учетные записи или API систем резервного копирования.



Минимизация рисков и реагирование на инциденты

Минимизация рисков

- Включает организационные и технические меры для предотвращения угроз.
- Основные меры: обучение персонала, ограничение доступа с принципом минимальных привилегий, шифрование данных и каналов передачи, мониторинг и контроль информационных ресурсов.
- Используются системы управления безопасностью, регулярные аудиты и инспекции, автоматизированные системы мониторинга (SIEM, DLP-системы и др.).
- Цель — снизить вероятность инцидента и минимизировать возможные потери при реализации рисков.



Как киберугрозы отражаются на бизнесе

Финансовые потери

Репутационный ущерб

Нарушение операционной деятельности

Рост затрат на защиту



Дополнительные риски

- ✓ Утечка коммерческой тайны и интеллектуальной собственности ведет к потере конкурентных преимуществ.
- ✓ Юридические последствия и судебные иски могут серьезно осложнять деятельность компании.
- ✓ Многочисленные «подписки на взлом» упрощают хакерам доступ к инструментам атак, увеличивая их частоту и опасность



ВЫВОД

Киберугрозы сегодня — это не абстрактная проблема, а ежедневная реальность любого бизнеса. Их невозможно полностью исключить, но грамотное управление рисками, обучение сотрудников, регулярный аудит ИТ-инфраструктуры и внедрение современных решений значительно снижают вероятность критических последствий.



Вы можете связаться со мной:

Тел: 8-923-502-95-59

E-mail: ner.kem@mail.ru

Telegram: [@VadCo1974](https://www.t.me/VadCo1974)

