**Лекция 9. Безопасность ИТ-инфраструктуры**

План:

### 1. Угрозы безопасности ИТ-инфраструктуры

### 2. Меры по обеспечению сетевой безопасности, безопасности баз данных, Web-приложений

3. Защита конфиденциальной информации в ИТ-инфраструктуре предприятия от несанкционированного доступа

### **1. Угрозы безопасности ИТ-инфраструктуры**

Сегодня часто в новостях появляется информация об утечках данных.

Для начала напомним, что в ИТ-инфраструктуру входят:

* сеть,
* серверы,
* клиентские устройства,
* мобильные устройства,
* ЦОДы.

Важно, чтобы эти компоненты исправно работали и были максимально защищены от атак. Чем больше элементов инфраструктуры взаимодействует между собой, тем выше риски и тем больше мер предосторожности должно быть. Если часть инфраструктуры будет скомпрометирована или выйдет из строя, под угрозой окажутся и другие связанные компоненты.

**В современном мире** **безопасность инфраструктуры – обязательное условие успешного существования любой компании**. Количество атак увеличивается с каждым годом. [По статистике](https://hightech.fm/2021/10/06/hacker-attack-year), за 9 месяцев 2021 года количество кибератак выросло на 54% по сравнению с тем же периодом 2020 года. Множественные утечки происходят у крупных компаний. Владельцы небольших компаний могут думать, что им ничего не грозит, но это не так. Ведь более 70 процентов атак нацелены именно на малый и средний бизнес. Внедрение технологий без обеспечения информационной безопасности чревато финансовыми и репутационными рисками для компании.

**Информационная безопасность ИТ-инфраструктуры нацелена на то, чтобы защитить инфраструктуру от атак злоумышленников, снизить вероятность технического сбоя, а также минимизировать финансовые последствия для бизнеса в случае атаки или сбоя**.

В безопасности ИТ-инфраструктуры нельзя один раз достичь требуемого уровня и оставить в таком состоянии. Эта сфера требует постоянного анализа актуальных угроз и критических уязвимостей. ***Поддержка безопасности среды ИТ-инфраструктуры должна быть постоянной.*** Стратегия защиты должна совершенствоваться, быть гибкой и меняться в соответствии с тенденциями атак и угроз.

## Что может угрожать безопасности инфраструктуры

**Наиболее распространенные угрозы безопасности:**

* **Фишинг**. Это самая распространённая угроза, которой подвержены как частные лица, так и организации. Главная цель фишинга – получить доступ к учётной записи сотрудника, которую затем злоумышленник использует для доступа к корпоративным ресурсам.
* **Программы-вымогатели**. Этот тип атаки характеризуется тем, что вредоносное ПО получает доступ к данным компании и шифрует их с целью получения выкупа. Уплата выкупа не гарантирует восстановление работы системы или отсутствие утечки данных. Такой тип атак встречается всё чаще.
* **Ботнет**. В основном используются для организации [DDoS-атак](https://www.reg.ru/blog/dos-vs-ddos-ataka-otlichiya-i-profilaktika/" \t "_blank). Но в последние годы ботнет стали использовать и для скрытого майнинга криптовалют. Для этого часто используется устройства IoT (интернет вещей).
* **Физическое вмешательство**. Инфраструктура компании может быть почти неуязвимой для кибератак, но нельзя забывать и о физической защите. Речь идёт о краже или проникновении на объект и физическом вмешательстве в работу оборудования.

## **Базовые правила безопасности**

## https://lh5.googleusercontent.com/DNUosjT7LyLWQd9gxVQHeuBxV_GC-aK5Q-EYcRhPS72Cdp_y-0kdVaVyoejLvuwKkzdWtNl04M5dy3q9GGAZLAY5Zph4dKZ9EKdNu6G3JrR5r7izdMn3I9kQbcCZfPHhhV7Zm6MI

Чтобы защитить инфраструктуру, нужно знать, каким угрозам может быть подвержена система. Можно читать отчёты по анализам актуальных угроз и использовать [сервисы информирования об угрозах](https://www.kaspersky.ru/enterprise-security/threat-intelligence).

Кроме этого, при проектировании и поддержке инфраструктуры стоит следовать общепринятым правилам безопасности:

* **удаляйте не используемое программное обеспечение и службы**. Активные, но простаивающие элементы создают дополнительную угрозу безопасности инфраструктуре;
* **установите  правильные настройки брандмауэра**. Неправильная конфигурация брандмауэра также опасна, как и его отсутствие;
* **настройте регулярное резервное копирование всех систем**. Это лучшая защита от программ-вымогателей;
* **проводите регулярное тестирование на проникновение и сканирование безопасности**. Это позволит найти уязвимые места в элементах системы;
* **при разработке кода проверяйте его на соответствие требованиям безопасности**. Для этого можно использовать DevSecOps. DevSecOps отвечает за включение требований по безопасности на всех этапах жизни разработки ПО;
* **используйте шифрование**. Не храните конфиденциальные данные в незашифрованном виде. Даже если злоумышленники получат доступ к данным, воспользоваться ими без ключей не получится;
* **следите за правами доступа пользователей**. Своевременно удаляйте права доступа у сотрудников, которые уволились;
* **установите парольные политики и строго следуйте им**.

Соблюдение даже этих базовых рекомендаций уже значительно повысит безопасность инфраструктуры.

Управление информационной безопасностью ИТ-инфраструктуры предприятия должно включать и работу с персоналом. Сотрудников компании стоит посвящать в вопросы кибербезопасности и рассказывать им о возможных угрозах. Крупные атаки и утечки данных зачастую начинаются с социальной инженерии.

Если сотрудники компании пользуются внутренними сервисами и имеют доступ к конфиденциальной информации, хорошим решением будет ***создание требований по информационной безопасности для персонала***. Цель — защита конфиденциальной информации и ИТ-инфраструктуры предприятия от несанкционированного доступа через устройства сотрудников.

Безопасный принцип работы на предприятии должен строиться на осведомленности сотрудников. Сетевая инфраструктура требует целостного подхода к текущим процессам и методам, чтобы гарантировать защищенность базовой инфраструктуры. Основные действия по защите объектов от угроз это:

1. Создание и поддержка процессов безопасного обмена данными между изолированными сетями.
2. Обеспечение надлежащих проверок состояния устройства для определения доступа к активам организации и отдельным сетям.
3. Обезвреживание вредоносного контента в файлах приложений или электронных письмах.

Усилия по защите ИТ-инфраструктуры направлены на снижение риска таких атак с помощью контрмер, таких как предотвращение и обнаружение вторжений, мониторинг безопасности, шифрование данных или управление конфигурацией.

Принципы кибербезопасности отображены на рисунке 1.

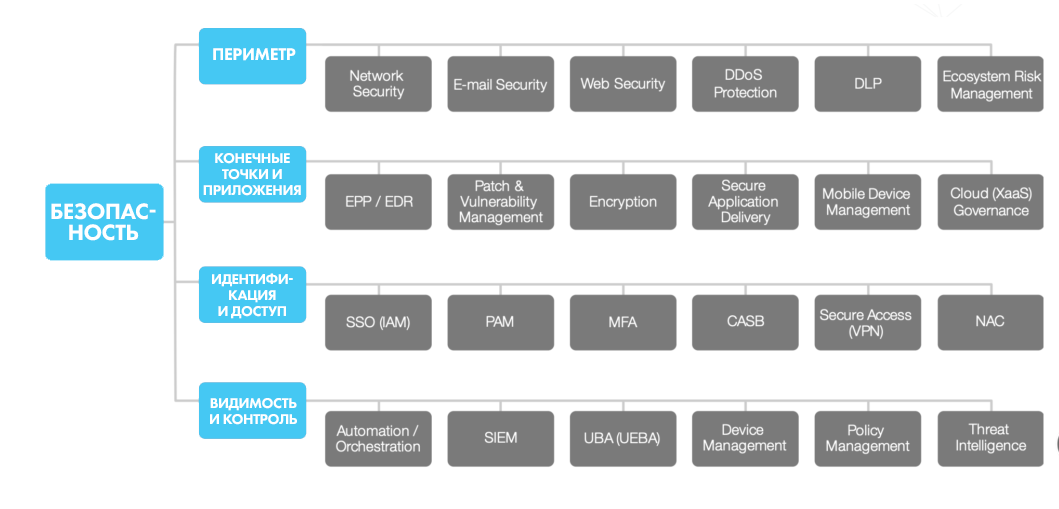


Рисунок 1. Принципы кибербезопасности

Плохое управление ИТ-инфраструктурой поставит под угрозу доход и репутацию бизнеса.

Большое количество физических атак или инцидентов, связанных с критически важной инфраструктурой во всем мире, демонстрирует уязвимость объектов КИИ. Поэтому им необходима оценка всего комплекса мер безопасности.

**Следующие подходы позволят реализовать защиту ИТ-инфраструктуры.**

**Безопасный доступ к устройствам инфраструктуры**. Разрешайте только доверенным пользователям доступ к ресурсам. Для обеспечения аутентичности пользователей путем реализации [многофакторной аутентификации (MFA)](https://cloudnetworks.ru/inf-bezopasnost/2fa/), [управления привилегированным доступом](https://cloudnetworks.ru/inf-bezopasnost/pim-pam-pum/) и [управления учетными данными администратора](https://cloudnetworks.ru/inf-bezopasnost/idm/).

**Ограничение ненужных коммуникаций**. Не упускайте одноранговые коммуникации в сети. Нефильтрованная связь между одноранговыми узлами позволит злоумышленникам свободно перемещаться и укрепляться в целевой сети, встраивая бэкдоры или устанавливая приложения.

**Повышение безопасности сетевых устройств**. Придерживайтесь отраслевых стандартов и передовых моделей в сетевом шифровании, защите доступа, политике паролей, ограничения физического доступа, резервного копирования конфигураций, периодического тестирования настроек безопасности и пр.

**Проверка целостности оборудования и ПО**. Продукты серого рынка угрожают ИТ-инфраструктуре, создавая вектор для атаки в сеть. Незаконные продукты могут быть предварительно загружены вредоносным программным обеспечением. Организации должны регулярно выполнять проверки целостности устройств и программного обеспечения.

**Сегментирование и разделение сетей и функций**. Уделите внимание общей структуре. Правильная сегментация и сегрегация ограничат распространение потенциальных злоумышленников на другие части внутренней сети. Оборудование (например, маршрутизаторов) создаст границы для фильтрации широковещательного трафика. Микросегменты будут ограничивать трафик или отключаться при обнаружении компьютерных атак. Виртуальное разделение по конструкции аналогично физическому.

**Управление сетью**. Реализуйте выделенные каналы связи для удаленного управления сетевыми устройствами, чтобы отделить пользовательский трафик и усилить безопасность сети. Так пользователи смогут безопасно обмениваться файлами во внутренней сети.

Защита критической инфраструктуры – это способность реагировать на серьезные инциденты, затрагивающие критическую инфраструктуру региона или страны. Секторы защиты критически важной инфраструктуры отображены на рисунке 2.



Рисунок 2. Секторы защиты информации

### **2. Меры по обеспечению сетевой безопасности, безопасности баз данных, Web-приложений**

# [**Защита сетевой инфраструктуры**](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/network-infrastructure-protection/)

**Сетевая инфраструктура** обеспечивает обмен информацией между пользователями и информационными системами, а также информационных систем между собой и тем самым выполняет важнейшую для нормального функционирования организации функцию – транспорта информации.

**Безопасность сетевой инфраструктуры**, обычно применяемая к корпоративным ИТ-средам, представляет собой *процесс защиты базовой сетевой инфраструктуры* путем установки превентивных мер для предотвращения несанкционированного доступа, модификации, удаления и кражи ресурсов и данных

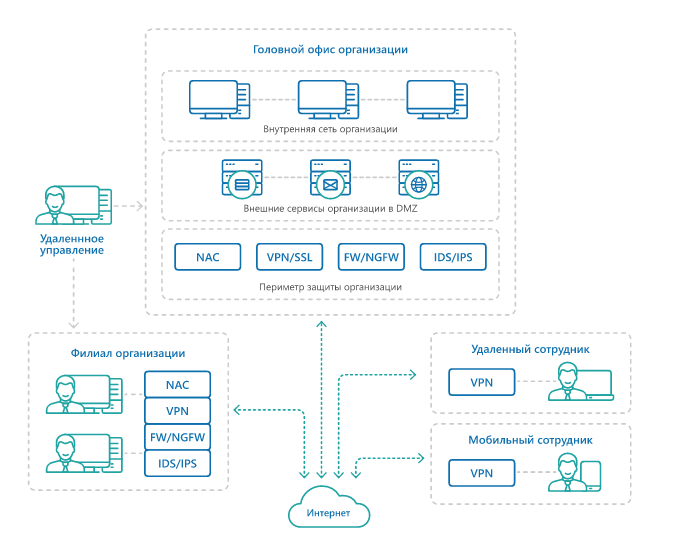


Рисунок 3. Безопасность сетевой инфраструктуры

**Основные меры:**

* защита от несанкционированного доступа путем фильтрации сетевых пакетов в соответствии с заданными правилами;
* разделение сети на сегменты по степени ограничения доступа к защищаемой информации, функциональному принципу и принципу обеспечения требуемого уровня информационной безопасности в каждом сегменте;
* обеспечение обнаружения преднамеренного несанкционированного доступа или специального воздействия на информационные ресурсы со стороны внешних нарушителей, действующих из внешних сетей, в том числе сети Интернет;
* обеспечение анализа трафика на наличие угроз, возникающих в сети, включая вредоносное поведение и аномалии в сетевом трафике;
* предоставление возможности расследования инцидентов ИБ, связанных с взаимодействием защищаемых сегментов с внешними сетями.

# [**Безопасность баз данных и приложений**](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/database-and-application-security/)

Непрерывность и качество работы бизнес-процессов заказчика напрямую зависят от работоспособности информационных систем. Именно поэтому на первый план выходит **задача защиты информационных систем и, в частности, их баз данных** (БД).

При этом межсетевых экранов или средств обнаружения/предотвращения компьютерных атак зачастую недостаточно, т.к. данные системы не позволяют отслеживать доступ непосредственно к самим данным, а также контролировать действия пользователей в системах с трехзвенной архитектурой (рисунок 4).

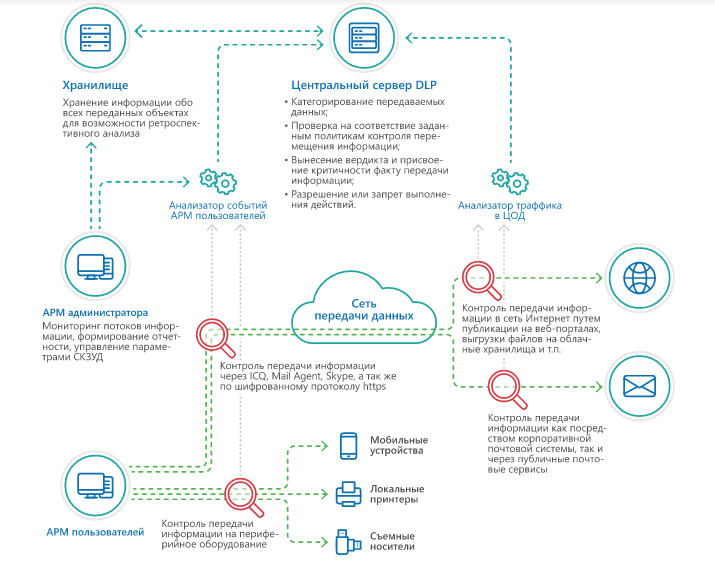


Рисунок 4. Безопасность баз данных и приложений

## **Основные меры к защите БД от внешнего и внутреннего злоумышленника, который заключается в проектировании и создании системы защиты web-приложений и БД, позволяющей заказчику:**

* осуществлять обнаружение и предотвращение несанкционированного доступа к web-приложениям и БД;
* создавать правила доступа к web-приложениям и системе управления базами данных (СУБД) на основе политик доступа к web-приложениям и СУБД;
* оперативно изменять правила доступа к web-приложениям и СУБД;
* выполнять централизованный мониторинг доступа к web-приложениям и СУБД;
* осуществить интеграцию средств системы защиты web-приложений и БД в существующую ИТ-инфраструктуру заказчика.

# [**Защита web-приложений**](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/web-application-security/)

Web-приложения, доступные из Интернета, являются привлекательной мишенью для злоумышленников.

Для атак на web-приложения злоумышленники используют различные техники и векторы атак. Необходимым звеном защиты web-ресурсов заказчика являются **межсетевые экраны web-приложений** (Web Application Firewall, WAF), т.к. только этот тип средств защиты позволяет обнаружить и предотвратить большинство типов атак, в том числе атаки на уровне бизнес-логики (рисунок 5).

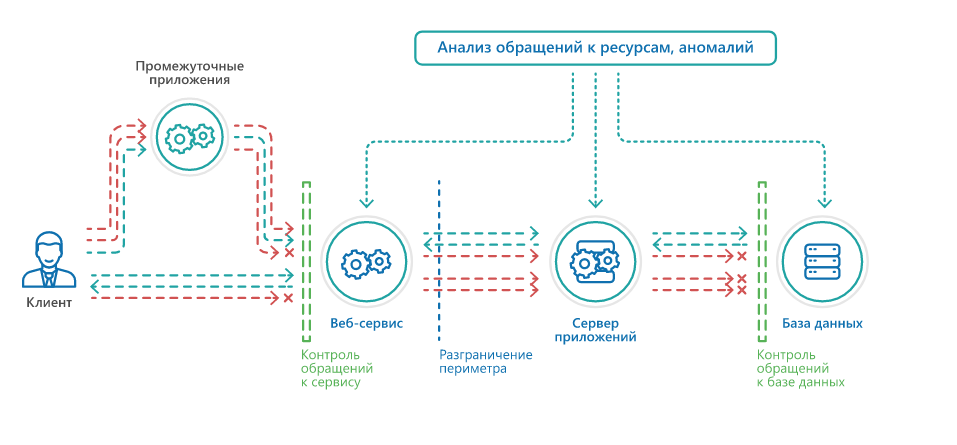


Рисунок 5. Защита web-приложений

## **Основные меры и способы защиты:**

* проверка данных на соответствие стандартам протоколов;
* самообучаемые механизмы проверки трафика, в т.ч. на основе нейронных сетей;
* сигнатурный анализ;
* защита от инъекций и XSS;
* защита от DDOS-атак;
* репутационный анализ;
* пользовательские правила обработки трафика.

# [**Безопасность ЦОД**](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/bezopasnost-cod/)

Современные центры обработки данных (ЦОД) сегодня представляют собой сложную разнородную среду, обеспечивающую поддержку многочисленных бизнес-критичных систем.

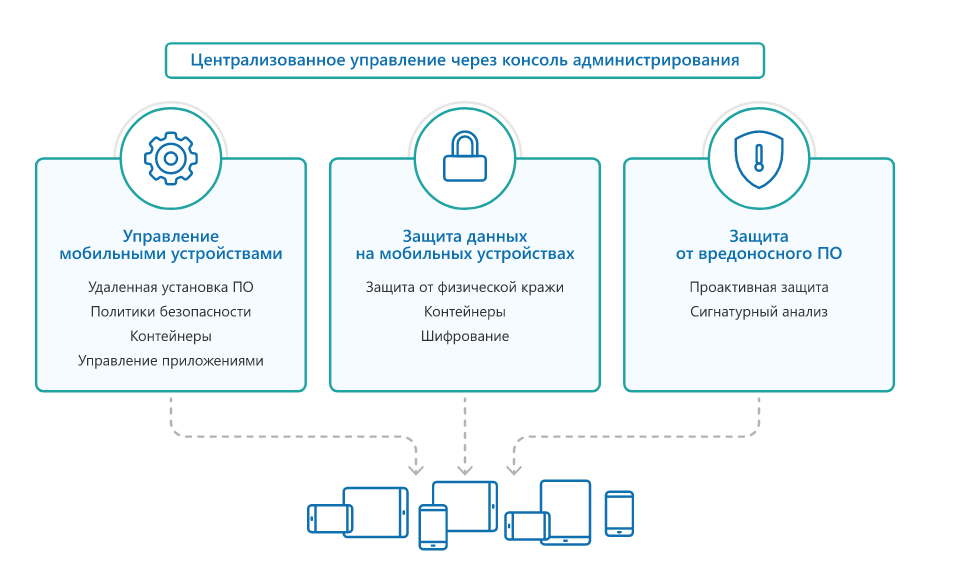
К особенностям таких ЦОД относятся территориальная распределенность, наличие гетерогенной аппаратной и программной инфраструктуры и высокая степень виртуализации.

## **Основные меры по обеспечению информационной безопасности центров обработки данных**

* разработка профилей безопасности для компонентов ИТ-инфраструктуры ЦОД с использованием встроенных механизмов защиты;
* проектирование и создание системы защиты информации для ЦОД и размещаемых в нем информационных ресурсов;
* аттестация ЦОД по требованиям безопасности информации.

# [**Безопасность мобильных устройств**](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/mobile-security/)

В связи с широким распространением мобильных устройств политика информационной безопасности многих заказчиков предполагает возможность доступа с указанных устройств к ресурсам корпоративной сети (рисунок 6).



# Рисунок 6. [Безопасность мобильных устройств](https://mte-cyber.by/services-and-solutions/it-infrastructure-security/mobile-security/)

**Основные меры**

 учет используемых устройств, управление конфигурациями операционных систем, управление мобильными приложениями (в том числе их инициализация и деинициализация, удаленная очистка, удаленный мониторинг и контроль за сбойными ситуациями);

 работу индивидуальных приложений в соответствии с корпоративными правилами (в том числе установка приложений из централизованного корпоративного репозитория и локального управления приложениями на устройстве);

 мобильную идентификацию, которая, в свою очередь, позволяет выполнять доступ к корпоративным приложениям только от «достоверных» устройств и пользователей;

 возможность безопасно сохранять на мобильном устройстве получаемую из внешних источников информацию (вложения в письма, файлы из каких-либо, в том числе облачных, репозиториев и пр.).

**3. Защита конфиденциальной информации в ИТ-инфраструктуре предприятия от несанкционированного доступа**

Конфиденциальная информация (данные) – это такая информация, доступ к которой ограничен согласно требованиям законодательства или нормами организации (предприятия) (рисунок 7).



Рисунок 7. Защита конфиденциальных данных

Требуют применения мер защиты следующие виды конфиденциальных данных:

* личные – касающиеся частной жизни граждан, в том числе [персональные данные (ПНд)](https://integrus.ru/blog/chto-otnositsya-k-personalnym-dannym-rossijskim-regulyatorom.html), за исключением сведений, подлежащих распространению в СМИ;
* служебные – то, что можно отнести к категории служебной тайны;
* судебные – любые сведения о судьях, должностных лицах контролирующих и правоохранительных органов, потерпевших, свидетелей, участников уголовного судопроизводства, а также любая информация из личных дел осужденных, о принудительном исполнении судебных актов;
* коммерческие – это коммерческая тайна, плюс сведения об изобретениях, полезных моделях, промышленных образцах до официальной публикации информации по ним предприятием (ноу-хау, технологии производства, секреты разработки и т.д.);
* профессиональные – врачебная, нотариальная, адвокатская тайна, тайна телефонных переговоров, почтовых сообщений, переписки, телеграфных и иных видов сообщений.

[**Защита данных и сведений в организации**](https://integrus.ru/blog/organizatsiya-obrabotki-zashhity-dannyh-na-predpriyatii.html)**строится на трех уровнях:**

1. ограничение несанкционированного доступа (с целью модификации, изменения, уничтожения, копирования, распространения и прочих неправомерных действий):
   * + замки, двери, решетки на окнах, сигнализация и т.д. — любые средства, ограничивающие физический доступ к носителям информации;
     + генераторы шума, сетевые фильтры и другие устройства, перекрывающие или обнаруживающие каналы утечки информации.
2. разграничение доступа для сотрудников (персонала) организации клиента;
3. реализация прав доступа для работников предприятия.

**Защита конфиденциальных данных предполагает проработку таких решений для ИТ-инфраструктуры, чтобы иметь возможность:**

* своевременного обнаружения фактов несанкционированного доступа к информации;
* снижения уязвимости технических средств обработки и хранения информации;
* оперативного восстановления поврежденной, модифицированной информации;
* предупреждения о последствиях несанкционированного доступа к конфиденциальным данным.

## **Средства защиты конфиденциальной информации**

Все средства и мероприятия, нацеленные на защиту конфиденциальной информации, базируются на трех уровнях:

1. **Правовой,** обеспечивающий единый госстандарт по информационной защите, но не нарушающий права пользователей. Уровень регламентируется Законом РК «Об информации, информатизации и защите информации», подзаконными актами РФ, внутриорганизационными положениями о защите конфиденциальной информации, определяющими работу с «закрытой» документацией. На этом уровне от нас требуется так выстроить информационную систему и решения по ее защите, чтобы не нарушить права пользователей и[нормы обработки данных](https://integrus.ru/blog/printsipy-obrabotki-personalnyh-dannyh.html).
2. **Организационный**, упорядочивающий работу с конфиденциальной документацией, определяющий степени и уровни доступа пользователей в информационные системы, носителями информации. Этот уровень предотвращает утечку сведений по халатности или небрежности персонала, сводя его к минимуму.
   * Архитектурно-планировочные мероприятия и решения, структурирование систем запросов и выдача допусков на пользование Интернетом, корпоративной электронной почтой, сторонними ресурсами.
   * Права на получение и использование подписи в электронном цифровом виде, следование корпоративным и морально-этическим правилам, принятым внутри организации, также являются важными составляющими защиты конфиденциальных данных.

3. [**Технический уровень защиты**](https://integrus.ru/blog/tehnicheskaya-zashhita-informatsii.html) конфиденциальной информации включает подуровни – аппаратный, криптографический, программный, физический.

### **Организация защиты конфиденциальных данных**

**1. Организационные мероприятия** по защите конфиденциальной информации начинаются с разработки регламента работы пользователей с информационной системой и информацией в ней. Правила доступа разрабатываются нашими специалистами совместно с руководством предприятия, службой безопасности.

**2. Уровни правовой и организационной защиты данных** являются неформальными [средствами защиты информации](https://integrus.ru/blog/metody-sredstva-tehnologii-zashhity-informatsii-v-seti-internet.html). Кроме административных (организационных) регламентов и законодательных (правовых) норм сюда можно отнести и морально-этические правила. Наша задача на административном уровне – пресечь, сделать невозможными повреждения или утечки данных вследствие нерадивости, халатности или небрежности персонала.

Решение поставленной задачи достигается за счет комплекса административных и технических мероприятий:

* разграничение и реализация прав доступа к конфиденциальным сведениям;
* защита переговорных комнат, кабинетов руководства от прослушки;
* оформление службы запросов на доступ к информационным ресурсам (внутренним и внешним);
* получение и обучение работы с электронными цифровыми подписями (ЭЦП).

### 3. Т**ехническая защита конфиденциальных сведений**

Физический, аппаратный, программный и криптографический уровни обеспечения защиты конфиденциальных данных относятся к формальным средствам. Это софт и «железо».

**Физический способ** предполагает поддержание работы механизмов, являющихся препятствием для доступа к данным вне информационных каналов: замки, видеокамеры, датчики движения/излучения и т.п. Это оборудование действует независимо от информационных систем, но ограничивает доступ к носителям информации.

**Аппаратными средствами безопасности** считаются все приборы, монтируемые в телекоммуникационных или информационных системах: спецкомпьютеры, серверы и сети организации, система контроля работников, шумовые генераторы, любое оборудование, перекрывающее возможные каналы утечек и обнаруживающее «дыры» и т.д.

**Программные средства** представляет комплексное решение, предназначенное для обеспечения безопасной работы (пример – DLP и SIEM системы, блокирующие возможную утечку данных и анализирующие реальные сигналы тревоги от устройств и приложений сетевого характера):

* DLP (Data Leak Prevention, предотвращение утечки данных) – средства для пресечения утечки данных, модификации информации, перенаправления информационных потоков;
* SIEM (Security Information and Event Management, управление событиями и информационной безопасностью) – анализ в режиме реального времени сигналов об угрозах, ведение журнала данных, создание отчетов. SIEM представлены приложениями, приборами, программным обеспечением.

**Криптографическая (математическая) защита** позволяет безопасно обмениваться данными в глобальной либо корпоративной сетях. Математические преобразованные, шифрованные каналы считаются оптимально защищенными. Но стопроцентной защиты никто гарантировать не может!

Криптография (шифрование) данных считается одним из самых надежных способов – технология сохраняет саму информацию, а не только доступ к ней. Средства шифрования обеспечивают защиту физических и виртуальных носителей информации, файлов и каталогов (папок), целых серверов.

Средства криптографической защиты конфиденциальной информации требуют внедрения программно-аппаратного комплекса:

* с использованием криптопровайдеров (программных компонентов шифрования);
* организацией VPN;
* применением средств формирования, контроля и использования ЭЦП.

При внедрении систем шифрования данных следует заранее продумать их совместимость с иными системами (включая внешние).

[Техническая защита конфиденциальной информации](https://integrus.ru/blog/tehnicheskaya-zashhita-personalnyh-dannyh.html) в организации требует проведения аттестации – набора организационных и иных мероприятий, достаточных для безопасной работы с конфиденциальными данными. Аттестация базируется на [требованиях и рекомендациях ФСТЭК](https://integrus.ru/blog/zashhita-informatsii-i-informatsionnaya-bezopasnost-fstek.html), применяется для защищаемых помещений и автоматизированных систем.

Отсутствие или недостаточное внимание к одной из составляющих защиты конфиденциальной информации на предприятии может закончиться тем, что внутренние данные окажутся достоянием мошенников. Обеспечивая информационную безопасность, необходимо всегда использовать комплексные меры, учитывающие множественность способов защиты.

<https://integrus.ru/blog/it-decisions/zashhita-konfidentsialnoj-informatsii-v-organizatsii.html>