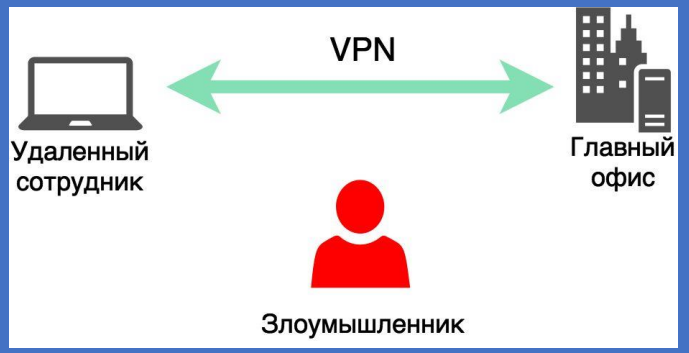
Проблемные вопросы обеспечения соответствия безопасного удаленного доступа к объектам КИИ

КОНСТАНТИН САМАТОВ

Члена Правления

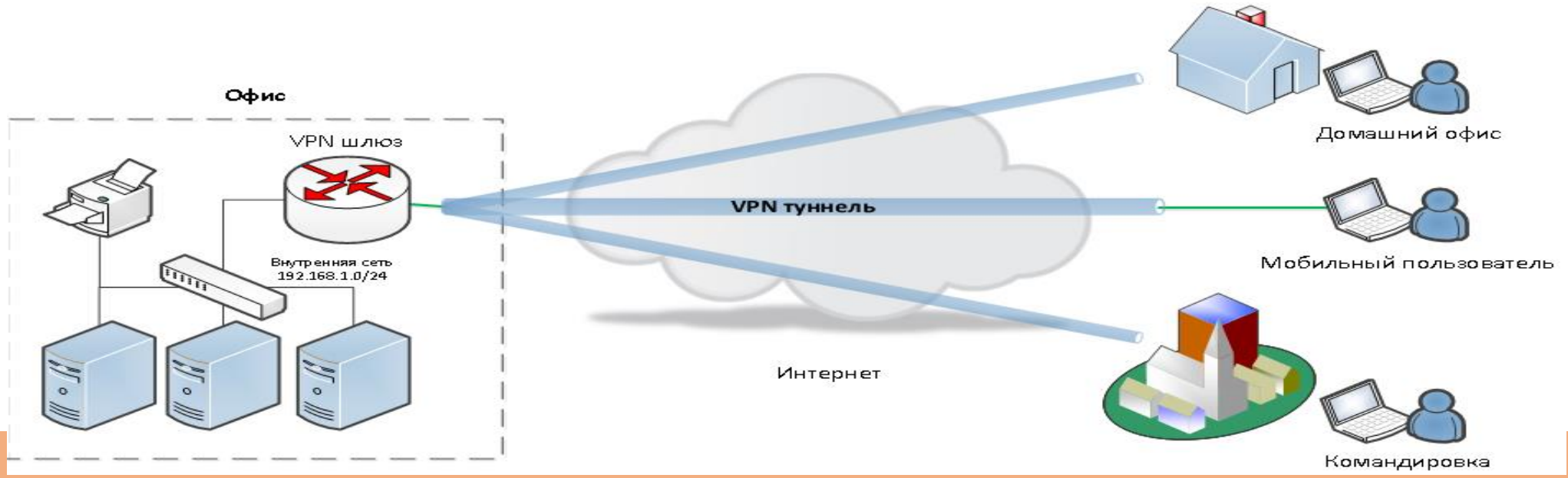
Ассоциации руководителей служб информационной безопасности

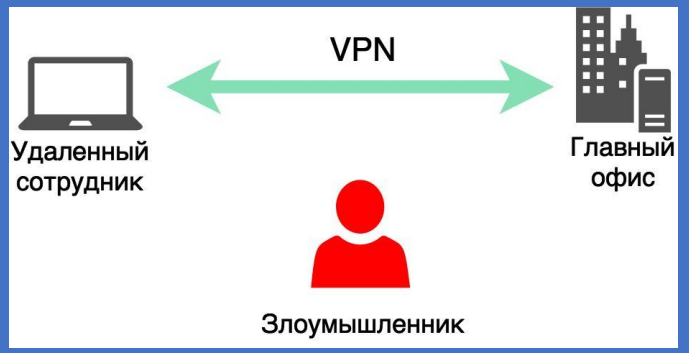


Вопрос 1. Что такое безопасный (защищенный) удаленный доступ?

Приложение № 1 к Мерам защиты информации в государственных информационных системах (Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г.)

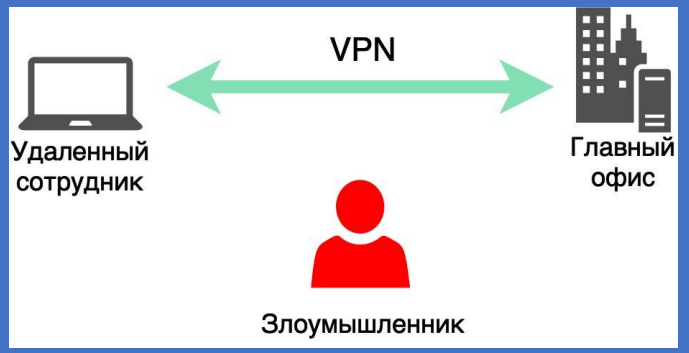
Удаленный доступ: процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически **<u>или логически</u>** с информационной системой, к которой он получает доступ.



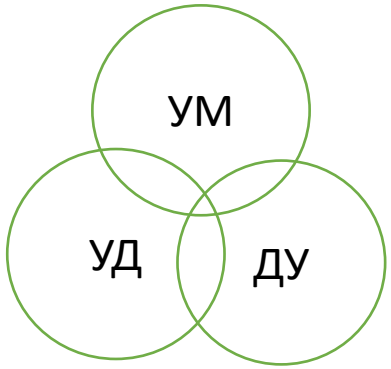


Вопрос 1. Что такое безопасный (защищенный) удаленный доступ?

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА ГОСТ Р 57429-2017	**Приложение № 1 к Мерам защиты информации в государственных информационных системах (Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г.)**
удаленный доступ: Процесс получения доступа к средствам вычислительной техники посредством вычислительной сети с использованием другого средства вычислительной техники.	Локальный доступ: доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).



Вопрос 1. Что такое безопасный (защищенный) удаленный доступ?



Дистанционное управление

Мониторинг информационной безопасности: Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГОСТ Р 59547-2021

Вопрос 2. Возможен ли ЗУД в КИИ?

- ОКИИ без КЗ – возможен
- Пункт 31 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. Приказом ФСТЭК России от 25.12.2017 № 239)
- В **значимом** объекте (КИИ) **не допускаются**:

наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, **не являющихся работниками** субъекта критической информационной инфраструктуры, а также работниками его дочерних и зависимых обществ;

- **В случае технической невозможности исключения** удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в значимом объекте **принимаются** организационные и технические **меры по обеспечению безопасности такого доступа.**

Вопрос 3. Разграничение ответственности при доступе к объектам КИИ?

- Законодательством о безопасности КИИ не предусмотрено
- Договорная ответственность в рамках гражданско-правовых отношений за вред причиненный действиями контрагента в форме возмещения убытков.
- Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации (Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

- Уголовный кодекс РФ

Часть 3 статьи 274.1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, **либо правил доступа** к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, **если оно повлекло причинение вреда** критической информационной инфраструктуре Российской Федерации

Спасибо за внимание!

КОНСТАНТИН САМАТОВ

Члена Правления

Ассоциации руководителей служб информационной безопасности