# Практическая методология создания и развития систем информационной безопасности (кейсы из личной практики)

**Докладчик**

**Трушкин Сергей Борисович**

# Преамбула

**Одним из направлений деятельности по повышению защищённости АИС является решение задачи обеспечения безопасного доступа субъектов к объектам доступа. Процесс аутентификации решает три подзадачи (AAA).**

- **Идентификация (предъявление признака субъекта доступа).**
- **Аутентификация (подтверждение признака субъекта доступа).**
- **Авторизация (многопользовательские системы).**

**Отсутствие комплексного подхода в решении задачи аутентификации в многопользовательских системах проявляется в понижение их информационной защищённости и возникновению (увеличению количества) рисков ИБ.**

**Разница подходов в построение и усиление защищённости ИС, выверенная методология или применение точечных мер на основе эвристического анализа ?**

# Аутентификация

**Целеполагание:**

- **Обеспечение защиты секретных реквизитов аутентификации субъекта доступа (закрытый ключ, биометрические данные и др.).**
- **Надлежащий уровень защиты прав и ролей доступа в информационной системе (защита соответствующих полей учётной записи субъекта).**
- **Определение подлинности субъекта и объекта доступа.**

**Реализация:**

- **Однофакторная, двухфакторная (обычная или строгая), трёхфакторная (как дополнительное усиление субъектности, представляемых реквизитов аутентификации доступа).**
- **Выбор методов распределения прав и ролей (например - дискретный, мандатный).**
- **Выбор метода определение подлинности субъекта и объектов доступа (односторонний, двухсторонний, трёхсторонний).**
- **Реализация решений по обеспечению безопасности технологической инфраструктуры.**

# Нормативные ориентиры

- **Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (Состав мер защиты информации и их базовые наборы для соответствующего класса защищённости информационной системы Раздел I. «Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ), II. Управление доступом субъектов доступа к объектам доступа (УПД)).**
- **Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014 г.**
- **Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» (с изменениями) предусматривает следующие виды электронной подписи.**
- **«Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом Гостехкомиссии России от 30.08.2002 №282.**
- **ГОСТ Р ИСО/МЭК 9594-8-98 — Основы аутентификации.**
- **FIPS 113 — COMPUTER DATA AUTHENTICATION**

# Методология

**Методологию создания, развития (усиления, модернизации) подсистем информационной безопасности в различных информационных системах состоит ряда последовательных взаимосвязанных этапов, на которых решаются целевые задачи на каждом этапе. При этом, результирующие сведения (данные) полученные на предыдущем этапе служат исходными решения целевых задач предыдущего этапа служат исходными данными для выполнения задач следующего этапа:**

- **Определение информационных активов, требующих защиты, исходя из требований законодательства или воли их владельца.**
- **Категорирование объекта информатизации, исходя из требований законодательства.**
- **Проведение обследования информационной системы.**
- **Формирование модели угроз ИБ. Оценка рисков ИБ.**
- **Определение класса информационной защищённости для ИС.**
- **Формирование технических решений, оценка соответствия выбранному классу защищённости.**
- **Построение системы защиты.**
- **Формирование политики информационной безопасности.**

# Идентификация активов, требующих защиты

**а) Государственной тайне.**

*РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) «Закон О государственной тайне».*

*Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 23.08.2018) «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.*

*Постановление Правительства РФ от 04.09.1995 N 870 (ред. от 18.03.2016) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».*

*Указ Президента РФ от 30.11.1995 N 1203 (ред. от 03.09.2018) «Об утверждении Перечня сведений, отнесенных к государственной тайне»*
*Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 29.12.2016) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».*

**Государственные регуляторы - ФСБ (8 Центр), МО (8 Управление), СВР. Контролирующий орган -** ФСБ России**. Ответственность -** уголовная и в отдельных случаях административная ответственность.

# Идентификация активов, требующих защиты

б) **Служебной тайне**.
*Постановление Правительства РФ от 03.11.1994 N 1233 (ред. от 18.03.2016) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».*
**Регуляторы и контролёры** – уполномоченные структуры в государственных организациях, органов государственного управления и т.д.
**Ответственность** в основном административная.

в) **Персональным данным**.
*Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ). Последние изменения введены в с 1марта 2021 г.*
**Государственные регуляторы** – ФСТЭК, ФСБ.
**Контролирующий орган** - Роскомнадзор.
**Ответственность** в основном административная.

# Идентификация активов, требующих защиты

**г) Коммерческой тайне.**

*Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне».*

**Регулятор и контролёр -** уполномоченное подразделение организации. Ответственность определяется в судебном порядке в зависимости от нанесённого ущерба.

**д) Банковской тайне.**

**Регулятор и контролёр** – ЦБ России.

# Объекты информатизации, требующие защиты в соответствии с требованиями законодательства

- **АИС в которых ведётся обработка информации, содержащей сведения о государственной и служебной тайне.**
- **Объекты КИИ.**
- **ИСПДн.**
- **ГИС и МИС.**
- **Объекты связи.**
- **Банковские  ИС и системы финансовых организаций.**

# Объекты информатизации, требующие защиты в инициативном порядке

- **Корпоративные ИС.**
- **Системы операторов (связи, ЦОД, обслуживающих организаций и т.д.) в соответствии с требованиями заключенных договорных взаимоотношений с Заказчиком.**

# Личные кейсы

- **Особенности реализация подсистемы аутентификации в АИС одной крупной интернациональной промышленной компании.**
- **Особенности реализации подсистемы аутентификации на объектах КИИ.**
- **Особенности реализации в АИС специализированного назначения.**

# Спасибо за внимание

**Трушкин Сергей**
**e-mail: Serg.Tr90@mail.ru**
**тел: 8 916 766 70 09**