Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Угрозы информационной безопасности

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

1. Угроза
Уязвимость
Риск

Уязвимость (брешь) (vulnerability)

- **Уязвимость** - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами [ГОСТ Р ИСО/МЭК 13335-1-2006];
- **Уязвимость** - это слабое звено информационной системы, которое, став известным злоумышленнику, может позволить ему нарушить ее безопасность.
- **Уязвимость - это потенциальный путь для выполнения атаки.**

- Уязвимости системы могут быть скрытыми, то есть еще не обнаруженными, известными, но только теоретически, или же общеизвестными и активно используемыми злоумышленниками.

- **Актив** - все, что имеет ценность для организации [ГОСТ Р ИСО/МЭК 13335-1-2006];

Уязвимость информации

- **Уязвимость информации** - возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации

- **Опасности**
  - Опасность физического уничтожения или искажения
  - Опасность несанкционированной модификации
  - Опасность несанкционированного получения
  - Опасность несанкционированного размножения (копирования)

Угроза (threat)

- **Угроза** - это действие или событие, способное нарушить безопасность информационных систем.

- **Угроза** потенциальная причина инцидента, который может нанести ущерб системе или организации [ГОСТ Р ИСО/МЭК 13335-1-2006];

- **Угроза** - набор обстоятельств и действий, которые потенциально могут привести к нарушению безопасности системы

- **Угроза ИБ** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 50922-2006];

Угрозы информационной безопасности

- Под **угрозой** принято понимать потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

- **Угроза (безопасности информации)** - это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

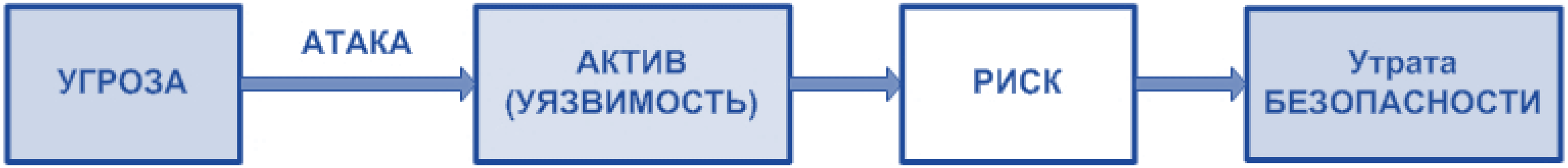
Угроза безопасности информации

- **Под угрозой безопасности информации** будем понимать возникновение такого явления или события, следствием которого могут быть негативные воздействия на информацию:
  - нарушение физической целостности,
  - нарушение логической структуры,
  - несанкционированная модификация, несанкционированное получение,
  - несанкционированное размножение.

- **Наиболее ощутимый ущерб связан с нарушением конфиденциальности**, когда сведения, предназначенные лишь для определенного круга лиц, попадают в посторонние руки.

Риск

- **Если уязвимость соответствует угрозе, то существует риск**
  (ИСО 2382-8:1998)



- **Риск - это сочетание угрозы и уязвимости.**
- **Угрозы без уязвимости не являются риском** так же, как и уязвимости без угроз. В реальном мире ни одно из этих условий не существует.
- **Атака (attack)** — это реализованная угроза

Взаимосвязь угроз ИБ с источниками, уязвимостью и рисками

- **Угрозы безопасности информации не возникают сами по себе.**
- **Угрозы всегда обусловлены уязвимостью информации**, проявляющуюся через уязвимость носителей информации, уязвимость информационной системы в которой защищаемая информация обрабатывается и наличием источника угрозы (от чего или от кого угроза исходит).

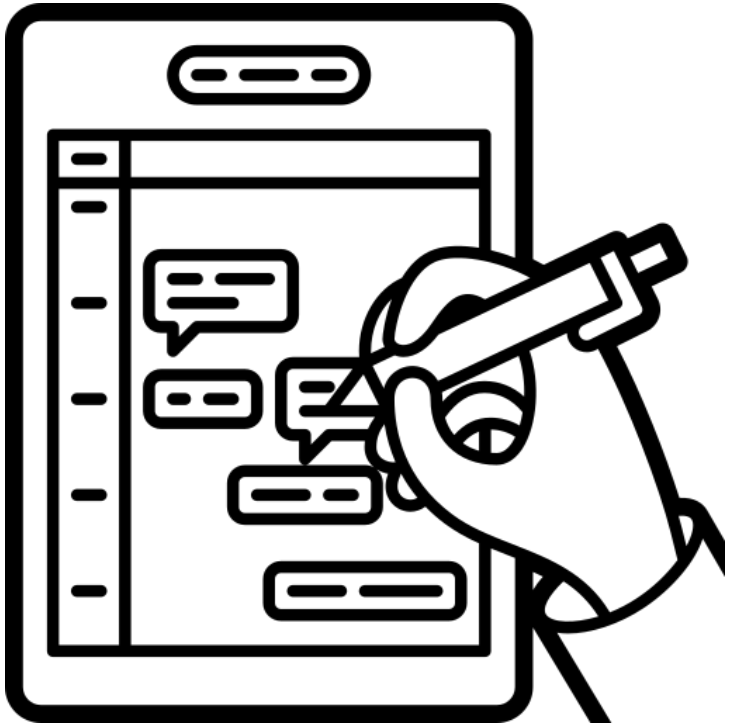
- **Уязвимость (информационной системы); брешь** – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

- **Если уязвимость соответствует угрозе, то существует риск.**

Оценка степени риска отвечает на вопрос «сколько средств нужно затратить на систему защиты» и сопоставить стоимость системы защиты со стоимостью (ценой, важностью) защищаемой информацией для нахождения оптимального в экономическом отношении решения.

Существует ряд подходов к измерению рисков. В методиках, рассчитанных на более высокие требования, используется **модель оценки риска с тремя факторами: угроза, уязвимость, цена потери.**


X3X3X3
В ФИЛЬМАХ
НАМ НАДО УДАЛИТЬ ДАННЫЕ С СЕРВЕРА
Я ВЗЛОМАЮ ЕГО СО СВОЕГО НОУТБУКА
В ЖИЗНИ
НАМ НАДО УДАЛИТЬ ДАННЫЕ С СЕРВЕРА
ЛЕГКО
VK.COM/XZXZ3



2. Задачи организационного обеспечения защиты информации

Защита информации (ЗИ)

- **Организационные мероприятия играют важную роль в создании надежного механизма защиты информации**, так как возможности несанкционированного использования конфиденциальных сведений зачастую обусловлены не только техническими аспектами, но и злоумышленными действиями, а также нерадивостью, небрежностью, халатностью пользователей или обслуживающего персонала, игнорирующего элементарные правила защиты.
- Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, ведомствах, учреждениях и организациях**.**
- **При рассмотрении вопросов ЗАЩИТЫ ИНФОРМАЦИИ (ЗИ) такая деятельность относится к организационным методам обеспечения.**

Организационное обеспечение ЗИ

- **Организационное обеспечение защиты информации (ЗИ)** — это регламентация производственной деятельности и взаимоотношений исполнителей, осуществляемая на нормативно-правовой основе таким образом, чтобы сделать невозможным или существенно затруднить разглашение, утечку и несанкционированный доступ к конфиденциальной информации за счет проведения соответствующих организационных мероприятий.

- **Цель применения организационных средств зашиты** состоит в том, чтобы исключить или, по крайней мере, свести к минимуму возможности реализации угроз информационной безопасности на **объектах обработки информации (ООИ).**

Организационное обеспечение ЗИ

- В информационных системах организационные мероприятия выполняют стержневую роль в реализации комплексной системы защиты информации.
- Только с их помощью возможно объединение на правовой основе инженерно-технических, программно-аппаратных, криптографических и других средств защиты информации в единую комплексную систему.

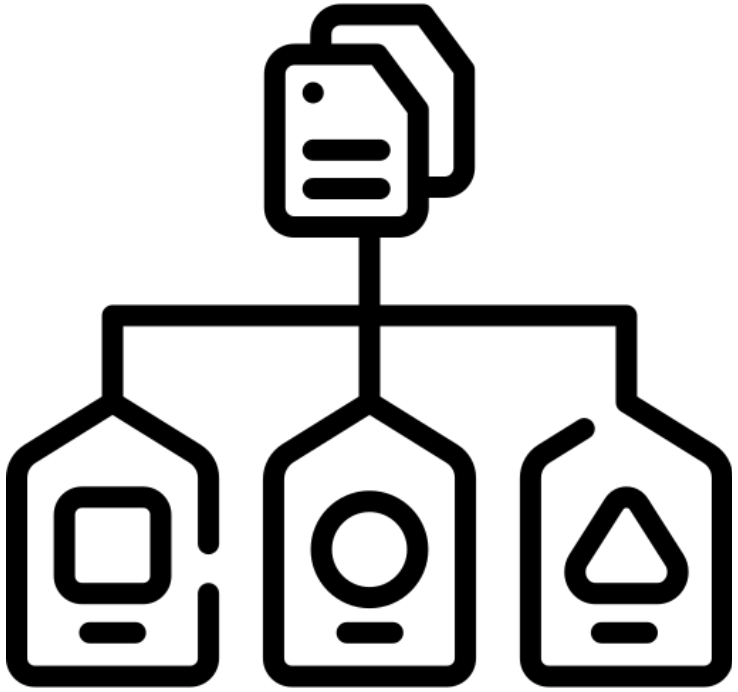
ЗАДАЧИ обеспечения безопасности функционирования информации на объекты обработки информации

На организационном уровне решаются следующие **задачи обеспечения безопасности функционирования информации на объекты обработки информации (ООИ)**:

- 1) организация работ по разработке системы защиты процессов переработки информации;
- 2) ограничение доступа на объект и к ресурсам ООИ;
- 3) разграничение доступа к ресурсам ООИ;
- 4) планирование мероприятий;
- 5) разработка документации;
- 6) воспитание и обучение обслуживающего персонала и пользователей;

ЗАДАЧИ обеспечения безопасности функционирования информации на объекты обработки информации

- 7) сертификация средств защиты процессов переработки информации;
- 8) лицензирование деятельности по защите процессов переработки информации;
- 9) аттестация объектов защиты;
- 10) совершенствование системы защиты процессов переработки информации;
- 11) оценка эффективности функционирования системы защиты процессов переработки информации;
- 12) контроль выполнения установленных правил работы на ООИ.



3. Классификация угроз информационной безопасности

Типы информационных угроз

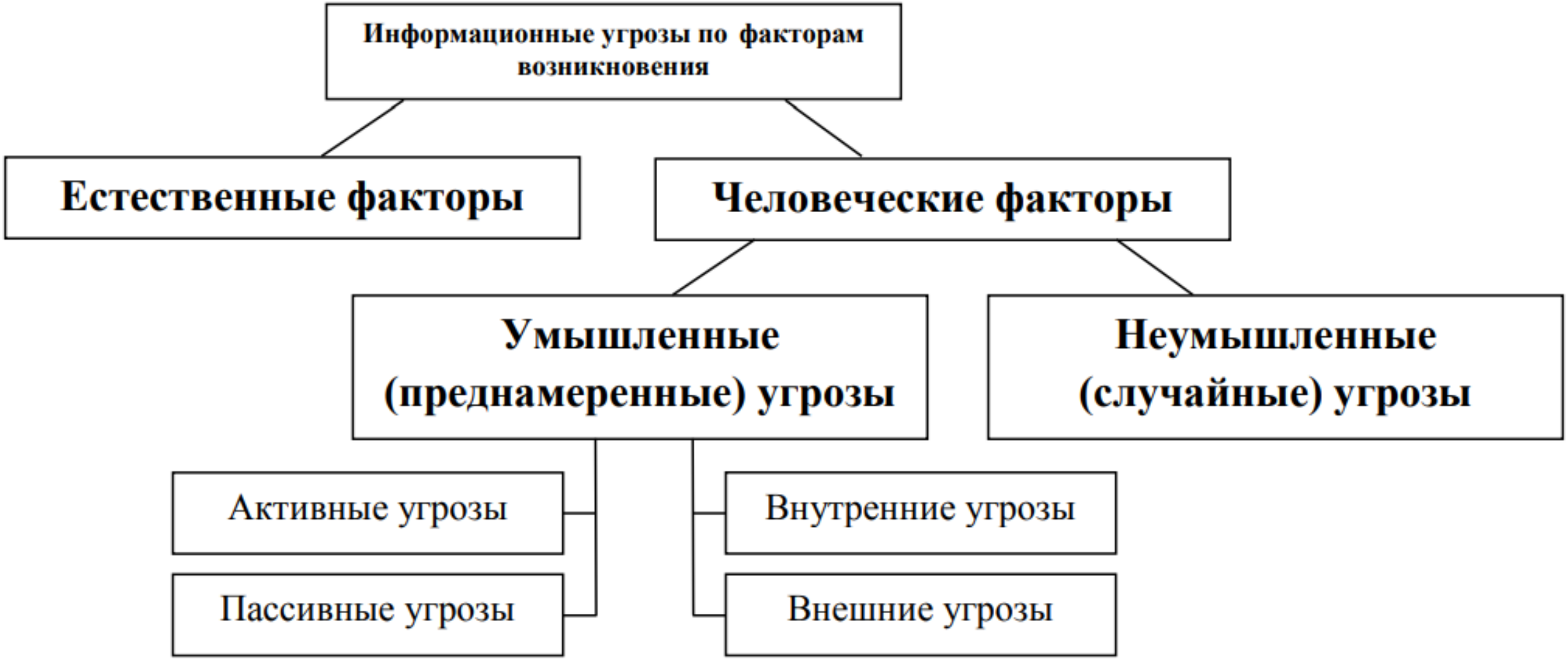
Классификация угроз информационной безопасности объектов обработки информации

- **Классификация** всех возможных **угроз** информационной безопасности (ИБ) объектов обработки информации (ООИ) может быть проведена **по ряду базовых признаков**.
  - 1. По природе возникновения.
  - 2. По степени преднамеренности появления.
  - 3. По непосредственному источнику угроз.
  - 4. По положению источника угроз.
  - 5. По степени зависимости от активности ООИ.
  - 6. По степени воздействия на ООИ.
  - 7. По способу доступа к ресурсам ООИ.
  - 8. По текущему месту расположения информации.

Классификация угроз
1. По природе возникновения

- **1. По природе возникновения.**
- **1.1. Естественные угрозы** — угрозы, вызванные воздействиями на объекты обработки информации объективных физических процессов или стихийных природных явлений, не зависящих от человека.
- **1.2. Искусственные угрозы**, т.е. угрозы, вызванные деятельностью человека.

Классификация угроз
1. По природе возникновения



Классификация угроз
2. По степени преднамеренности появления.

- **2. По степени преднамеренности появления.**
- **2.1. Угрозы умышленные** (преднамеренные), обусловленные злоумышленными действиями людей.
- **2.2. Угрозы случайного действия** (естественные), т.е. не зависящие от воли людей.


Угрозы ИБ
Умышленные факторы
Хищение носителей информации
Подключение к каналам связи
Перехват ЭМИ
Несанкционированный доступ
Разглашение информации
Копирование данных
Шпионаж и диверсии
Вредительные программы
Случайные факторы
Несчастные случаи
Пожары
Аварии
Взрывы
Стихийные бедствия
Ураганы
Наводнения
Землетрясения
Ошибки в процессе обработки информации
Ошибки пользователя
Ошибки оператора
Сбои аппаратуры

Классификация угроз
2. По степени преднамеренности появления.

- **Угрозы, связанные с ошибками в процессе обработки информации** могут быть следующими:
  - проявление ошибок программно-аппаратных средств объектов обработки информации;
  - некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
  - неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
  - неправомерное включение оборудования или изменение режимов работы устройств и программ;
  - неумышленная порча носителей информации;
  - пересылка данных по ошибочному адресу абонента (устройства);
  - ввод ошибочных данных;
  - неумышленное повреждение каналов связи.

Классификация угроз
3. По непосредственному источнику угроз.

- **3. По непосредственному источнику угроз.**
- 3.1. Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение).
- 3.2. Угрозы, непосредственным источником которых является человек.
- 3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.
- 3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

Классификация угроз
3. По непосредственному источнику угроз.

- 3. По непосредственному источнику угроз.
- **3.2. Угрозы, непосредственным источником которых является человек**, например:
  - **введение агентов в число персонала системы** (в том числе, возможно, и в административную группу, отвечающую за безопасность);
  - **вербовка** (путем подкупа, шантажа) персонала или отдельных пользователей, имеющих определенные полномочия;
  - **угроза несанкционированного копирования** секретных данных пользователем объектов обработки информации;
  - **разглашение**, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков).

Классификация угроз
3. По непосредственному источнику угроз.

- 3. По непосредственному источнику угроз.
- **3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства**, например:
  - **запуск технологических программ**, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
  - **возникновение отказа в работе операционной системы**.

Классификация угроз
3. По непосредственному источнику угроз.

- 3. По непосредственному источнику угроз.
- **3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства**, например:
  - **нелегальное внедрение и использование неучтенных программ** (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
  - **заражение компьютера вирусами** с деструктивными функциями.

Классификация угроз
4. По положению источника угроз.

- **4. По положению источника угроз.**
- 4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится объект обработки информации (ООИ).
- 4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится ООИ.
- 4.3. Угрозы, источник которых имеет доступ к периферийным устройствам ООИ (терминалам).
- 4.4. Угрозы, источник которых расположен на ООИ.

Классификация угроз
4. По положению источника угроз.

- 4. По положению источника угроз.
- **4.1. Угрозы, источник которых расположен вне контролируемой зоны территории** (помещения), на которой находится объект обработки информации, например:
  - **перехват побочных электромагнитных, акустических и других излучений устройств и линий связи**, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
  - **перехват данных, передаваемых по каналам связи**, и их анализ в целях выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
  - **дистанционная фото- и видеосъемка**.

Классификация угроз
4. По положению источника угроз.

- 4. По положению источника угроз.
- **4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения),** на которой находится объект обработки информации, например:
  - **хищение производственных отходов** (распечаток, записей, списанных носителей информации и т.п.);
  - **отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем** (электропитания, охлаждения и вентиляции, линий связи и т.д.);
  - **применение подслушивающих устройств**.

Классификация угроз
4. По положению источника угроз.

- 4. По положению источника угроз.
- **4.3. Угрозы, источник которых имеет доступ к периферийным устройствам объектов обработки информации (ООИ) (терминалам).**

- **4.4. Угрозы, источник которых расположен на ООИ**, например:
  - проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
  - некорректное использование ресурсов ООИ.

Классификация угроз
5. По степени зависимости от активности ООИ

- **5. По степени зависимости от активности объектов обработки информации (ООИ).**
- **5.1. Угрозы, которые могут проявляться независимо от активности ООИ**, например:
  - вскрытие шифров криптозащиты информации;
  - хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).
- **5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных** (например, угрозы выполнения и распространения программных вирусов).

Классификация угроз
6. По степени воздействия на ООИ

- **6. По степени воздействия на объекты обработки информации (ООИ).**
- **6.1. Пассивные угрозы**, которые при реализации ничего не меняют в структуре и содержании ООИ (например, угроза копирования секретных данных).
- **6.2. Активные угрозы**, которые при воздействии вносят изменения в структуру и содержание ООИ, например:
  - **внедрение аппаратных спец. вложений, программных «закладок» и вирусов** («троянских коней» и «жучков»), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам в целях регистрации и передачи критической информации или дезорганизации функционирования системы;
  - **действия по дезорганизации функционирования системы** (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
  - **угроза умышленной модификации информации**.

Классификация угроз
7. По способу доступа к ресурсам ООИ

- **7. По способу доступа к ресурсам ООИ.**
- **7.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам ООИ**, например:
  - **незаконное получение паролей и других реквизитов разграничения доступа** (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя;
  - **несанкционированное использование терминалов пользователей**, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.
- **7.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам ООИ**, например:
  - **вход в систему в обход средств зашиты** (загрузка посторонней операционной системы со сменных магнитных носителей и др.);
  - **угроза несанкционированного доступа к ресурсам ООИ** путем использования недокументированных возможностей ОС.

Классификация угроз
8. По текущему месту расположения информации.

- **8. По текущему месту расположения информации.**
- **8.1. Угрозы доступа к информации на внешних запоминающих устройствах** (например, угроза несанкционированного копирования секретной информации с жесткого диска).
- **8.2. Угрозы доступа к информации в оперативной памяти**.
- **8.3. Угрозы доступа к информации, циркулирующей в линиях связи**.
- **8.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере** (например, угроза записи отображаемой информации на скрытую видеокамеру).

Классификация угроз
8. По текущему месту расположения информации.

- 8. По текущему месту расположения информации.
- **8.3. Угрозы доступа к информации, циркулирующей в линиях связи**, например:
  - **незаконное подключение к линиям** связи в целях работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
  - **незаконное подключение к линиям связи в целях прямой подмены** законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
  - **перехват всего потока данных** в целях дальнейшего анализа не в реальном масштабе времени.

Обеспечение свойств информации

- Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации **объект обработки информации удовлетворяет потребности эксплуатирующих его лиц, если обеспечиваются следующие свойства информации и систем ее обработки:**
  1. целостность,
  2. конфиденциальность
  3. и доступность.

ИБ обеспечивается если

- В соответствии с существующими подходами принято считать, что **информационная безопасность объектов обработки информации обеспечена в том случае, если** для любых информационных ресурсов объекта **поддерживается**
  1. **определенный уровень целостности** (невозможности несанкционированной или случайной модификации информации),
  2. **конфиденциальности** (невозможности несанкционированного получения какой-либо информации)
  3. и **доступности** (возможности за разумное время получить требуемую информацию).

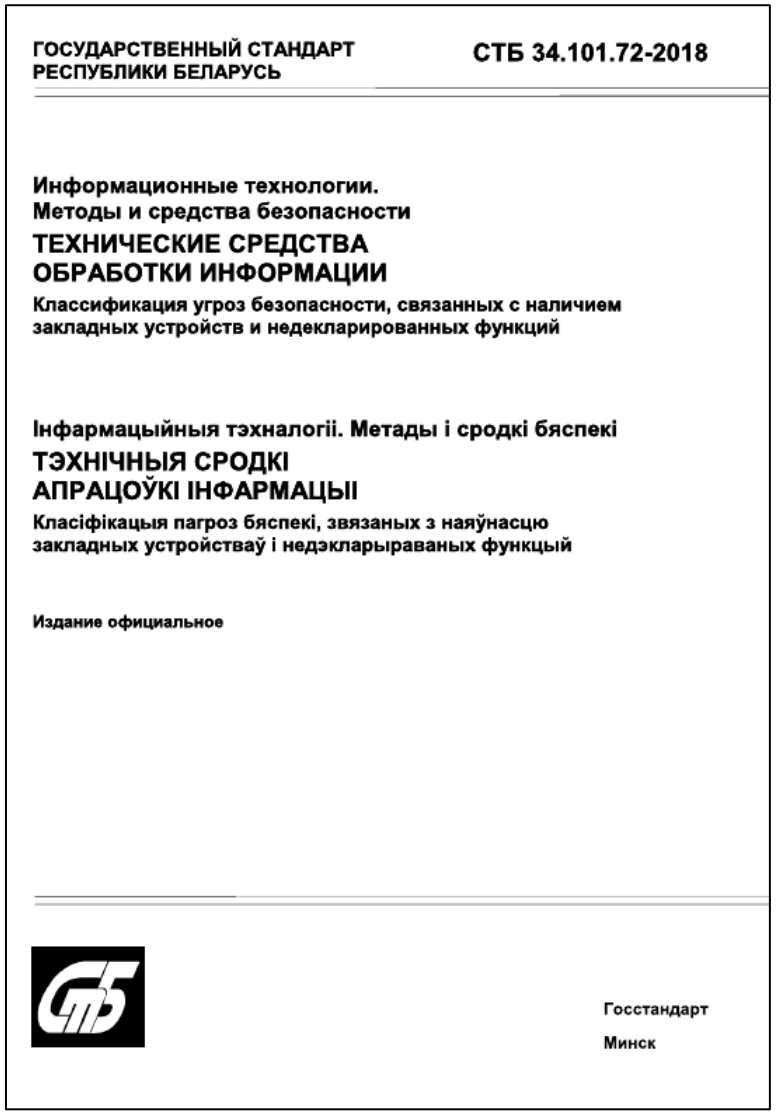
Основные виды угроз

- Соответственно для объектов обработки информации (ООИ) рассматриваются основные виды угроз:
  - **Угроза нарушения целостности** включает в себя любое умышленное изменение информации, хранящейся на ООИ или передаваемой из одной системы в другую.
  - **Угроза нарушения конфиденциальности** заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней.
  - **Угроза нарушения доступности (ограничения доступа)** возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу ООИ.
  - **Угроза раскрытия параметров ОИИ**, когда злоумышленник знает все параметры системы информационной безопасности организации и может их обойти.

4. Классификация угроз в соответствии с СТБ 34.101.72-2018

СТБ 34.101.72-2018
Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. ***Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций***

СТБ 34.101.72-2018



ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ 34.101.72-2018

Информационные технологии.
Методы и средства безопасности
ТЕХНИЧЕСКИЕ СРЕДСТВА
ОБРАБОТКИ ИНФОРМАЦИИ
Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций

Інфармацыйныя тэхналогіі. Метады і сродкі бяспекі
ТЭХНІЧНЫЯ СРОДКІ
АПРАЦОЎКІ ІНФАРМАЦЫІ
Класіфікацыя пагроз бяспекі, звязаных з наяўнасцю закладных устройстваў і недэкларыраваных функцый

Издание официальное

Госстандарт
Минск

СТБ 34.101.72-2018 Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. **Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций**

Настоящий стандарт устанавливает классификацию угроз безопасности, связанных с наличием закладных устройств и (или) недекларированных функций в технических средствах, предназначенных для обработки информации, подлежащей защите в соответствии с законодательством Республики Беларусь, в том числе информации, распространение и (или) предоставление которой ограничено, на объектах информатизации.

СТБ 34.101.72-2018
Требования настоящего стандарта применяют при:

- **разработке политики информационной безопасности организации**, эксплуатирующей технические средства обработки информации, для идентификации активов и угроз, оценки рисков безопасности организации в целях принятия решения о необходимости принятия мер (применения средств управления) согласно требованиям СТБ ISO/IEC 27001;
- **реализации мер защиты информации на объектах информатизации от угроз безопасности**, связанных с наличием закладных устройств и (или) недекларированных функций в технических средствах обработки информации, согласно требованиям Указа Президента Республики Беларусь «О некоторых мерах по совершенствованию защиты информации» от 16 апреля 2013 г. № 196;
- **разработке и актуализации обобщенной модели угроз** применения закладных устройств и недекларированных функций в технических средствах обработки информации;
- **разработке и актуализации частных моделей угроз** применения закладных устройств и недекларированных функций в конкретных технических средствах обработки информации.

СТБ 34.101.72-2018 Классификация угроз

- **К основным признакам угроз безопасности**, связанным с наличием закладных устройств и недекларированных функций (НФ) в технических средствах обработки информации (ТСОИ), относятся:
  - тип актива, на который направлена угроза;
  - тип характеристики актива, на изменение которой направлена угроза.

- **К вспомогательным признакам угроз безопасности**, связанным с наличием закладных устройств и НФ в ТСОИ, относятся:
  - источник реализации угрозы;
  - этап жизненного цикла ТСОИ, на котором осуществляется внедрение закладных устройств или НФ;
  - вид мер защиты, уязвимости которых используют закладные устройства или НФ;
  - направление воздействия;
  - этап жизненного цикла ТСОИ, на котором осуществляется реализация угрозы.

СТБ 34.101.72-2018

- **Угрозы безопасности, связанные с наличием закладных устройств и недекларированных функций в технических средствах обработки информации (ТСОИ)**, подразделяются на следующие подклассы **по типу актива ТСОИ:**
- **а) угрозы безопасности информации:**
  - 1) угрозы обрабатываемой информации;
  - 2) угрозы технологической информации;
  - 3) угрозы информации механизмов защиты, в том числе системы защиты информации объектов информатизации;
- **б) угрозы безопасности ресурсов:**
  - 1) угрозы программных средств;
  - 2) угрозы аппаратных (аппаратно-программных) средств.

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств и недекларированных функций в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по типу характеристики актива ТСОИ:**
- **а) угрозы, направленные на нарушение свойств актива:**
  - 1) угрозы конфиденциальности информации;
  - 2) угрозы целостности информации;
  - 3) угрозы доступности информации;
  - 4) угрозы целостности ресурсов (конфигурации аппаратных и программных средств);
- **б) угрозы, направленные на нарушение выполняемых активом функций:**
  - 1) угрозы нарушения производительности ресурсов (программных, аппаратных (аппаратно-программных) средств);
  - 2) угрозы доступности ресурсов:
    - угрозы сбоя аппаратных (аппаратно-программных) средств;
    - угрозы отказа аппаратных (аппаратно-программных) средств.

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств и недекларированных функций в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по источнику реализации:**
- **а) угрозы, реализующиеся посредством воздействия от субъекта:**
  - 1) угрозы, реализующиеся сигналом управления из-за пределов ТСОИ;
  - 2) угрозы, реализующиеся путем непосредственного физического доступа к ТСОИ;
- **б) угрозы, реализующиеся без воздействия субъекта:**
  - 1) угрозы, реализующиеся при изменении логического состояния или режима работы ТСОИ при обработке информации;
  - 2) угрозы, реализующиеся при изменении физических параметров ТСОИ;
  - 3) угрозы, реализующиеся при изменении параметров внешней среды.

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств (ЗУ) и недекларированных функций (НФ) в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по этапу жизненного цикла ТСОИ, на котором осуществляется внедрение ЗУ или НФ:**
- **а) угрозы, возникающие в результате внедрения ЗУ или НФ на этапе разработки и создания ТСОИ:**
  - 1) угрозы внесения ЗУ или НФ в конструкторскую документацию на этапе проектирования ТСОИ;
  - 2) угрозы внесения ЗУ или НФ при технологическом процессе производства ТСОИ без внесения изменений и дополнений в конструкторскую документацию;
- **б) угрозы, возникающие в результате внедрения ЗУ или НФ на этапе поставки и установки ТСОИ:**
  - 1) угрозы внесения ЗУ или НФ на этапе транспортировки ТСОИ;
  - 2) угрозы внесения ЗУ или НФ на этапе установки и настройки ТСОИ;
- **в) угрозы, возникающие в результате внедрения ЗУ или НФ на этапе эксплуатации и сопровождения ТСОИ:**
  - 1) угрозы внесения ЗУ или НФ во время эксплуатации ТСОИ;
  - 2) угрозы внесения ЗУ или НФ во время проведения работ по обслуживанию или модернизации ТСОИ сторонними организациями.

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств (ЗУ) и недекларированных функций (НФ) в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по виду мер защиты, уязвимости которых использует ЗУ или НФ:**
- **а) угрозы, использующие уязвимости правовых мер защиты: угрозы, реализующиеся в результате отсутствия или несоблюдения нормативных правовых актов, в том числе ТНПА, в области защиты информации (информационной безопасности);**
- **б) угрозы, использующие уязвимости организационных мер защиты:**
  - 1) угрозы, реализующиеся в результате несанкционированного доступа лиц на ОИ либо несанкционированного перемещения технических средств в пределы границ ОИ;
  - 2) угрозы, реализующиеся в результате несоблюдения политик безопасной эксплуатации ОИ;
- **в) угрозы, использующие уязвимости технических мер защиты:**
  - 1) угрозы, реализующиеся путем использования уязвимостей в настройке программных и (или) технических средств защиты или ввиду их отсутствия;
  - 2) угрозы, реализующиеся путем использования нетрадиционных каналов связи (скрытые каналы передачи данных, побочные технические каналы утечки).

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств и недекларированных функций в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по направлению воздействия:**
  - угрозы, направленные на нарушение характеристик активов ТСОИ;
  - угрозы, направленные на нарушение характеристик активов, принадлежащих другим ТСОИ.

СТБ 34.101.72-2018

- Угрозы безопасности, связанные с наличием закладных устройств и недекларированных функций в технических средствах обработки информации (ТСОИ), подразделяются на следующие подклассы **по этапу жизненного цикла ТСОИ или ОИ, на котором осуществляется реализация угроз:**
  - угрозы, реализующиеся на этапе создания ТСОИ;
  - угрозы, реализующиеся на этапе поставки и установки ТСОИ;
  - угрозы, реализующиеся на этапе эксплуатации и сопровождения ТСОИ;
  - угрозы, реализующиеся на этапе вывода из эксплуатации ТСОИ.

Рекомендации по учету подклассов угроз

Основные признаки		Вспомогательные признаки													
Тип актива	Тип характеристики актива	Источник реализации угрозы		Этап жизненного цикла ТСОИ, на котором осуществляется внедрение ЗУ или НФ			Вид мер защиты, уязвимости которых используют ЗУ или НФ			Направление воздействия		Этап жизненного цикла ТСОИ, на котором осуществляется реализация угрозы			
		Реализующиеся посредством воздействия от субъекта	Реализующиеся без воздействия субъекта	Возникающие на этапе разработки и создания	Возникающие на этапе поставки и установки	Возникающие на этапе эксплуатации и сопровождения	Уязвимости правовых мер защиты	Уязвимости организационных мер защиты	Уязвимости технических мер защиты	Нарушение характеристик активов ТСОИ	Нарушение характеристик активов, принадлежащих другим ТСОИ	Реализующиеся на этапе создания	Реализующиеся на этапе поставки и установки	Реализующиеся на этапе эксплуатации и сопровождения	Реализующиеся на этапе вывода из эксплуатации
Обрабатываемая информация	Конфиденциальность	+	+	+	+	+	+	+	+	+	+		+	+	+
	Целостность	+	+	+	+	+	+	+	+	+	+		+	+	+
	Доступность	+	+	+	+	+	+	+	+	+	+		+	+	+
Технологическая информация	Конфиденциальность	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	Целостность	+	+	+	+	+	+	+	+	+	+	+	+	+	
	Доступность	+	+	+	+	+	+	+	+	+	+	+	+	+	
Информация механизмов защиты	Конфиденциальность	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	Целостность	+	+	+	+	+	+	+	+	+	+	+	+	+	
	Доступность	+	+	+	+	+	+	+	+	+	+	+	+	+	
Программные средства	Целостность	+	+	+	+	+	+	+	+	+	+		+	+	
	Производительность	+	+	+	+	+	+	+	+	+	+		+	+	
	Доступность	+	+	+	+	+	+	+	+	+	+		+	+	
Аппаратные (аппаратно-программные) средства	Целостность	+	+	+	+	+	+	+	+	+	+	+	+	+	
	Производительность	+	+	+	+	+	+	+	+	+	+	+	+	+	
	Доступность	+	+	+	+	+	+	+	+	+	+	+	+	+	

Примечание – Знак «+» означает, что при формировании семейств угроз учитывается вспомогательный признак.

5. Угрозы в информационной сфере в соответствии с Концепцией национальной безопасности Республики Беларусь и Концепцией информационной безопасности Республики Беларусь

Информационная безопасность *– состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;*

Концепция национальной безопасности Республики Беларусь

https://pravo.by/document/?guid=3871&p0=P223s0001

Концепция национальной безопасности Республики Беларусь

- **37. В информационной сфере внутренними источниками угроз национальной безопасности являются:**
- распространение недостоверной или умышленно искаженной информации, способной причинить вред национальным интересам Республики Беларусь;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить вред национальной безопасности;
- несоответствие качества национального контента мировому уровню;
- активное использование информационно-коммуникационных технологий для совершения правонарушений;
- расширение возможностей для неправомерных действий в отношении персональных данных;
- недостаточная эффективность информационного обеспечения государственной политики;
- низкий уровень правосознания и безопасного поведения пользователей информационно-коммуникационных технологий;
- нарушение установленного порядка обращения с государственными секретами.

https://pravo.by/document/?guid=3871&p0=P223s0001

Концепция национальной безопасности Республики Беларусь

- **46. В информационной сфере внешними источниками угроз национальной безопасности являются:**
- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
- целенаправленная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая вред национальным интересам Республики Беларусь в информационной сфере, в первую очередь по формированию негативного образа государства в мире;
- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
- препятствование распространению национального контента Республики Беларусь за рубежом;
- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
- несовершенство механизмов международного сотрудничества в противодействии преступности с использованием информационно-коммуникационных технологий.

https://pravo.by/document/?guid=3871&p0=P223s0001

Концепция национальной безопасности Республики Беларусь

- **Важнейшими направлениями нейтрализации внутренних источников угроз национальной безопасности в информационной сфере являются:**
- обеспечение защиты персональных данных от несанкционированного или случайного доступа к ним, иных неправомерных действий;
- противодействие деструктивному информационному воздействию, наносящему вред национальным интересам;
- информационное обеспечение и сопровождение государственной политики, в том числе информационное противоборство для защиты информационного пространства;
- развитие массового политического сознания граждан;
- усиление позитивного восприятия Беларуси в мировом информационном пространстве;
- дальнейшая реализация стратегии по формированию в Республике Беларусь информационного общества, гарантированное обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, получение информационных услуг;

https://pravo.by/document/?guid=3871&p0=P223s0001

Концепция национальной безопасности Республики Беларусь

- **Важнейшими направлениями нейтрализации внутренних источников угроз национальной безопасности в информационной сфере являются:**
- динамичное внедрение информационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества, в том числе методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны;
- создание комплексной цифровой инфраструктуры для межведомственного информационного взаимодействия;
- формирование современной системы оказания государственных услуг на принципах проактивности и мультиканальности их предоставления;
- развитие национальной системы обеспечения кибербезопасности;
- профилактика, выявление и пресечение правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
- совершенствование системы защиты информации и сведений, составляющих охраняемую законодательством тайну.

https://pravo.by/document/?guid=3871&p0=P223s0001

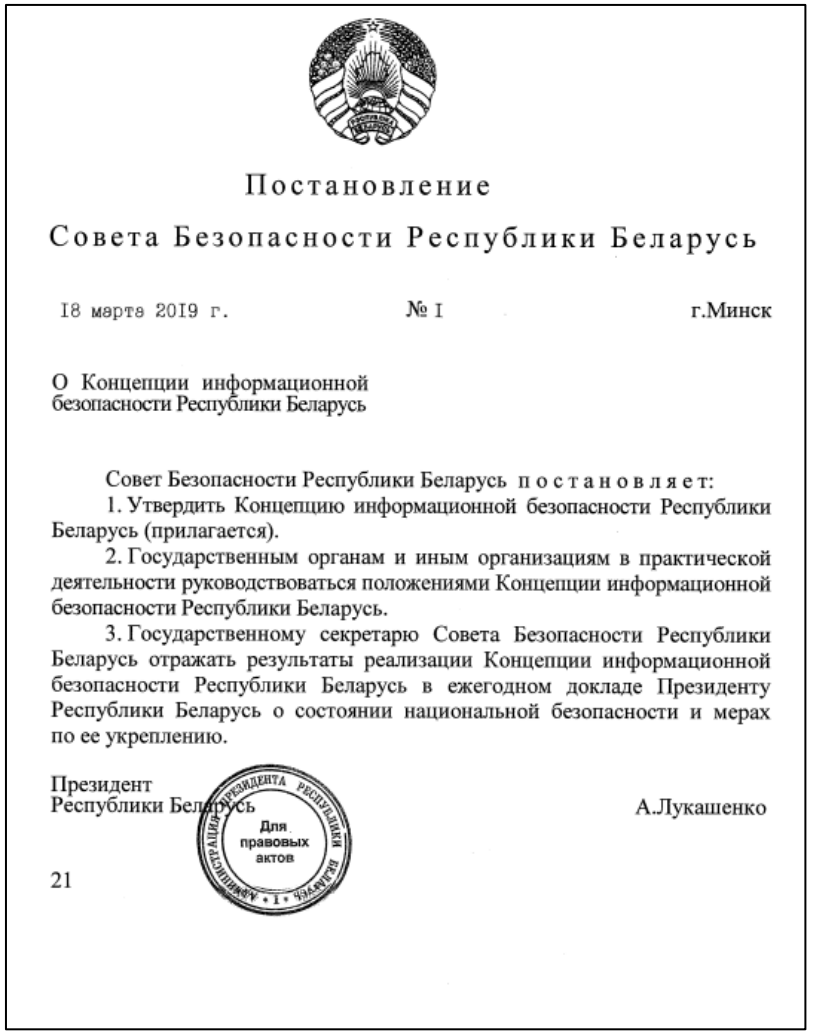
Концепция национальной безопасности Республики Беларусь

- **Меры по защите от внешних источников угроз национальной безопасности в информационной сфере осуществляются путем:**
- участия Республики Беларусь в формировании механизмов международного и регионального сотрудничества по противодействию преступности с использованием информационно-коммуникационных технологий исходя из национальных интересов;
- создания и безопасного использования межгосударственных, международных глобальных информационных сетей и систем;
- сокращения использования иностранных информационных технологий.

https://pravo.by/document/?guid=3871&p0=P223s0001

Постановление Совета Безопасности Республики Беларусь 18.03.2019 № 1

Концепция информационной безопасности Республики Беларусь



Постановление

Совета Безопасности Республики Беларусь

18 марта 2019 г. № 1 г.Минск

О Концепции информационной безопасности Республики Беларусь

Совет Безопасности Республики Беларусь п о с т а н о в л я е т:

1. Утвердить Концепцию информационной безопасности Республики Беларусь (прилагается).

2. Государственным органам и иным организациям в практической деятельности руководствоваться положениями Концепции информационной безопасности Республики Беларусь.

3. Государственному секретарю Совета Безопасности Республики Беларусь отражать результаты реализации Концепции информационной безопасности Республики Беларусь в ежегодном докладе Президенту Республики Беларусь о состоянии национальной безопасности и мерах по ее укреплению.

Президент Республики Беларусь А.Лукашенко

Для правовых актов

21

- **Концепция информационной безопасности Беларуси** – это система официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, в которой определяются стратегические задачи и приоритеты в области обеспечения информационной безопасности.
- Документ обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере, способствует целенаправленной интеграции Беларуси в системы обеспечения международной информационной безопасности на основе национальных приоритетов.
- В Концепции отражены современные вызовы и угрозы, которые формируются в информационной сфере и представляют опасность для конституционных основ и жизнедеятельности государств - манипулирование массовым сознанием, дискредитация идеалов и ценностей, размывание национального суверенитета, неустойчивость информационной инфраструктуры и другие.
- http://mininform.gov.by/upload/medialibrary/6f8/6f80a36dcb2aac3bcaa330cda20ae733.pdf
- https://pravo.by/document/?guid=3871&p0=P219s0001

Концепция информационной безопасности РБ

- **ГЛАВА 9 ГОСУДАРСТВЕННОЕ РЕАГИРОВАНИЕ НА РИСКИ, ВЫЗОВЫ И УГРОЗЫ В ИНФОРМАЦИОННОЙ СФЕРЕ**
- 33. Государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия.
- Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государство в лице этих государственных органов и организаций обеспечивает своевременное принятие мер безопасности, незамедлительно оповещает заинтересованные субъекты, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

- 34. Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба). Определяется защищенность и устойчивость объектов информационной безопасности, в том числе информационной инфраструктуры, информационных ресурсов, индивидуального, группового и массового сознания к действию угроз. Выявляются и исключаются условия возникновения и реализации рисков, вызовов и угроз информационной безопасности.

https://pravo.by/document/?guid=3871&p0=P219s0001

Концепция информационной безопасности РБ

- 35. Подготавливаются и внедряются сценарии и планы кризисного реагирования на кибератаки, компьютерные инциденты, акты деструктивного информационного воздействия, иные угрозы информационной безопасности, а также проводятся учения и тренировки сил реагирования.
- Реализуется политика информационного сдерживания, выражающаяся в демонстрации достоверной готовности к отражению деструктивных информационных воздействий, достаточной возможности технологического, организационного, правового противодействия угрозам в информационной сфере и выявления их источников.

- 36. В случае существенного осложнения информационной обстановки, связанного в том числе с необходимостью обеспечения военной безопасности государства, осуществляются дополнительные меры защиты информационной сферы правовыми, информационно-технологическими, техническими и иными методами (информационное противоборство), обеспечивается приоритетное взаимодействие военной организации государства и гражданского сектора.

- 37. Вооруженные Силы Республики Беларусь, иные воинские формирования предпринимают меры по обеспечению информационной безопасности в рамках решения возложенных задач по своему непосредственному предназначению с применением современных, высокотехнологичных сил и средств.

- 38. Беларусь участвует в международном реагировании на потенциальные риски, вызовы и угрозы информационной безопасности в рамках заключенных договоров и соглашений, осуществляет межгосударственное взаимодействие в анализе рисков, вызовов и угроз информационной безопасности, обмен опытом и совместные практические мероприятия.

https://pravo.by/document/?guid=3871&p0=P219s0001

Концепция информационной безопасности РБ

- 61. **В качестве наиболее вероятных источников угроз кибербезопасности рассматриваются** отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, противоправная деятельность отдельных лиц и преступных групп, преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации, зависимость Беларуси от других стран – производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры

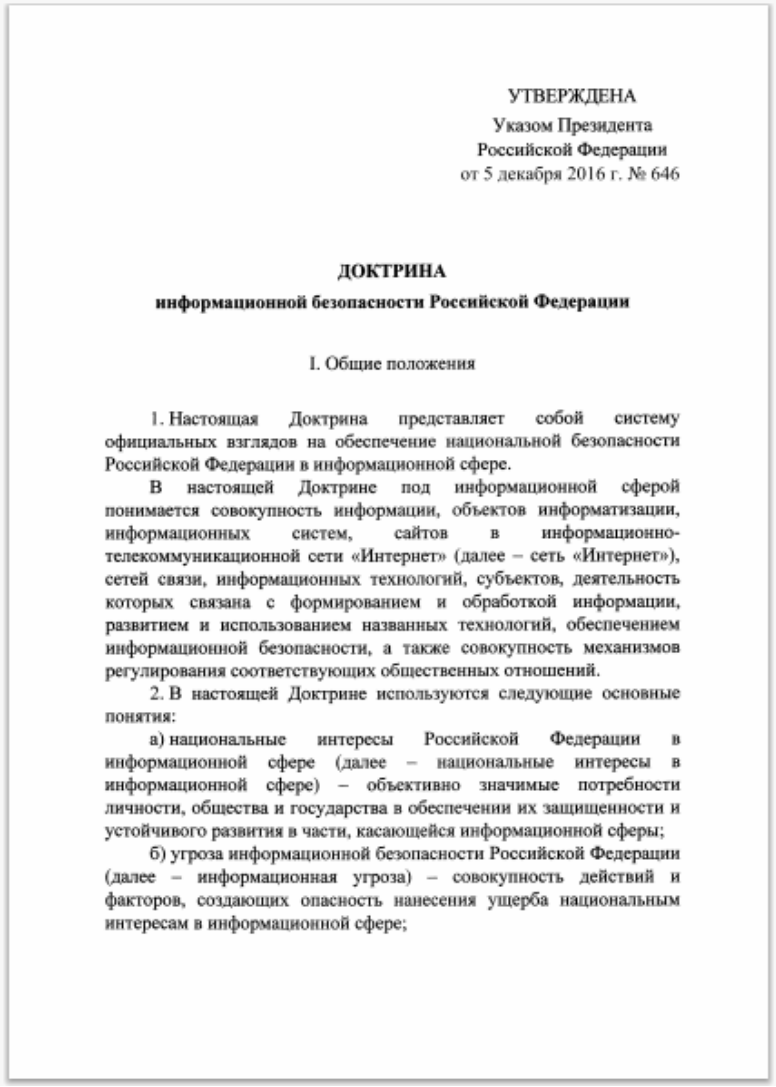
https://pravo.by/document/?guid=3871&p0=P219s0001

Указом Президента РФ
№ 646 от 5 декабря 2016 г.
Доктрина
информационной
безопасности
Российской Федерации

6. Угрозы в информационной сфере в соответствии с Доктриной информационной безопасности Российской Федерации

Информационная безопасность Российской Федерации *- состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;*

Доктрина информационной безопасности Российской Федерации



УТВЕРЖДЕНА
Указом Президента
Российской Федерации
от 5 декабря 2016 г. № 646

ДОКТРИНА
информационной безопасности Российской Федерации

I. Общие положения

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

2. В настоящей Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации в информационной сфере (далее – национальные интересы в информационной сфере) – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

- **Доктрина информационной безопасности Российской Федерации** (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)
- В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.
- http://www.scrf.gov.ru/security/information/document5/
- http://static.kremlin.ru/media/events/files/ru/tGeA1AqAfJ4uy9jAOF4CYCpuLQw1kxdR.pdf

III. Основные информационные угрозы и состояние информационной безопасности

- **10. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.**
- Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.
- При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

- **11. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.**
- Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

III. Основные информационные угрозы и состояние информационной безопасности

- **12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия**, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.
- Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.
- Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.
- **13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание** в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

III. Основные информационные угрозы и состояние информационной безопасности

- **14. Возрастают масштабы компьютерной преступности**, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.
- **15. Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях**, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

III. Основные информационные угрозы и состояние информационной безопасности

- **16. Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры**, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.
- **17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий** и их использования для производства продукции и оказания услуг. Остается **высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий** в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

III. Основные информационные угрозы и состояние информационной безопасности

- **18. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий**, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.
- **19. Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.**
- Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.
- Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

7. Угрозы в информационной сфере в соответствии с Конвенцией ООН об обеспечении международной информационной безопасности

Концепция Конвенции ООН об обеспечении международной информационной безопасности
http://www.scrf.gov.ru/security/information/document112/
https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Основные угрозы и факторы, влияющие на обеспечение международной информационной безопасности

- **1. Использование информационно-коммуникационных технологий в военно-политических целях**, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.
- **2. Использование информационно-коммуникационных технологий в террористических целях**, в том числе для проведения компьютерных атак на объекты информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников.
- **3. Использование информационно-коммуникационных технологий для вмешательства во внутренние дела суверенных государств**, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию, а также для нанесения вреда общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Основные угрозы и факторы, влияющие на обеспечение международной информационной безопасности

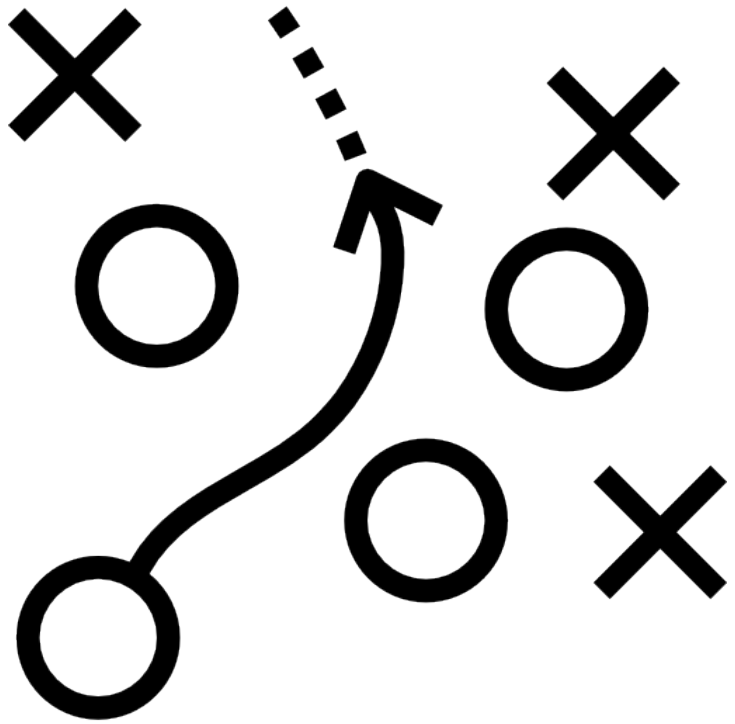
- **4. Использование информационно-коммуникационных технологий для совершения преступлений**, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.
- **5. Использование информационных ресурсов, находящихся под юрисдикцией другого государства**, без согласования с компетентными структурами этого государства.
- **6. Распространение вредоносного программного обеспечения и информации**, противоречащей принципам и нормам международного права, а также национальным законодательствам государств.
- **7. Использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека**, реализуемым в информационном пространстве, прежде всего праву человека на уважение его личной (частной) жизни.
- **8. Нарушение безопасного, непрерывного и стабильного функционирования сети «Интернет»**.

Основные угрозы и факторы, влияющие на обеспечение международной информационной безопасности

- **9. Противодействие доступу к новейшим информационно-коммуникационным технологиям**, создание условий технологической зависимости в сфере информатизации.
- **10. Включение в информационно-коммуникационные технологии и средства недекларируемых возможностей**, а также сокрытие производителями информации об уязвимостях в их продуктах.
- **11. Недостаточная оценка возникающих угроз информационной безопасности**, связанных с внедрением новых технологий, таких как искусственный интеллект, «большие данные», интернет вещей, блокчейн и другие.
- **12. Использование технологического доминирования для монополизации различных сегментов рынка информационно-коммуникационных технологий**, включая основные информационные ресурсы, критическую инфраструктуру, ключевые технологии, продукты и услуги, а также для препятствования осуществлению независимого контроля и проведению мероприятий, направленных на обеспечение информационной безопасности.

Основные угрозы и факторы, влияющие на обеспечение международной информационной безопасности

- **13. Допущение использования государствами своей информационной инфраструктуры для совершения международно-противоправных деяний**, а также использование государствами посредников, в том числе негосударственных субъектов, для совершения таких деяний.
- **14. Публичное распространение под видом достоверных сообщений заведомо ложной информации**, приводящее к возникновению угрозы жизни и безопасности граждан или к наступлению тяжких последствий.
- **15. Невозможность точной идентификации источника компьютерных атак или ложной информации**, обусловленная технологическими особенностями информационно-коммуникационных технологий, а также отсутствием организационных механизмов обеспечения деанонимизации информационного пространства.



8. Основные направления и методы реализации угроз

Основные направления реализации злоумышленником информационных угроз

- **К основным направлениям реализации злоумышленником информационных угроз относятся:**
  - непосредственное обращение к объектам доступа;
  - создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
  - модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
  - внедрение в технические средства программных или технических механизмов, нарушающих предполагаемую структуру и функции системы.

Основные методы реализации угроз информационной безопасности

- **К числу основных методов реализации угроз информационной безопасности относятся:**

1. определение злоумышленником типа и параметров носителей информации;
2. получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;
3. получение злоумышленником детальной информации о функциях, выполняемых системой;
4. получение злоумышленником данных о применяемых системах защиты;

Основные методы реализации угроз информационной безопасности

5. определение способа представления информации;
6. определение злоумышленником содержания данных, обрабатываемых в системе, на качественном уровне (применяется для мониторинга и для дешифрования сообщений);
7. хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;
8. использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок;
9. уничтожение средств вычислительной техники и носителей информации;

Основные методы реализации угроз информационной безопасности

10. несанкционированный доступ пользователя к ресурсам системы в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;
11. несанкционированное превышение пользователем своих полномочий;
12. несанкционированное копирование программного обеспечения;
13. перехват данных, передаваемых по каналам связи;
14. визуальное наблюдение;
15. раскрытие представления информации (дешифрование данных);

Основные методы реализации угроз информационной безопасности

16. раскрытие содержания информации на семантическом уровне;
17. уничтожение носителей информации;
18. внесение пользователем несанкционированных изменений в программно-аппаратные компоненты системы и обрабатываемые данные;
19. установка и использование нештатного аппаратного и/или программного обеспечения;
20. заражение программными вирусами;
21. внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;

Основные методы реализации угроз информационной безопасности

22. внедрение дезинформации;
23. выведение из строя носителей информации без уничтожения;
24. проявление ошибок проектирования и разработки аппаратных и программных компонентов;
25. искажение соответствия синтаксических и семантических конструкций языка;
26. запрет на использование информации.

Действия и события, нарушающие информационную безопасность

Умышленные или неосторожные действия сотрудников, приведшие к ознакомлению с КИ недопущенных лиц

Выражается в:
– сообщении;
– передаче;
– предоставлении;
– пересылке;
– опубликовании;
– утере
И иных способах
Реализуется по каналам распространения и СМИ

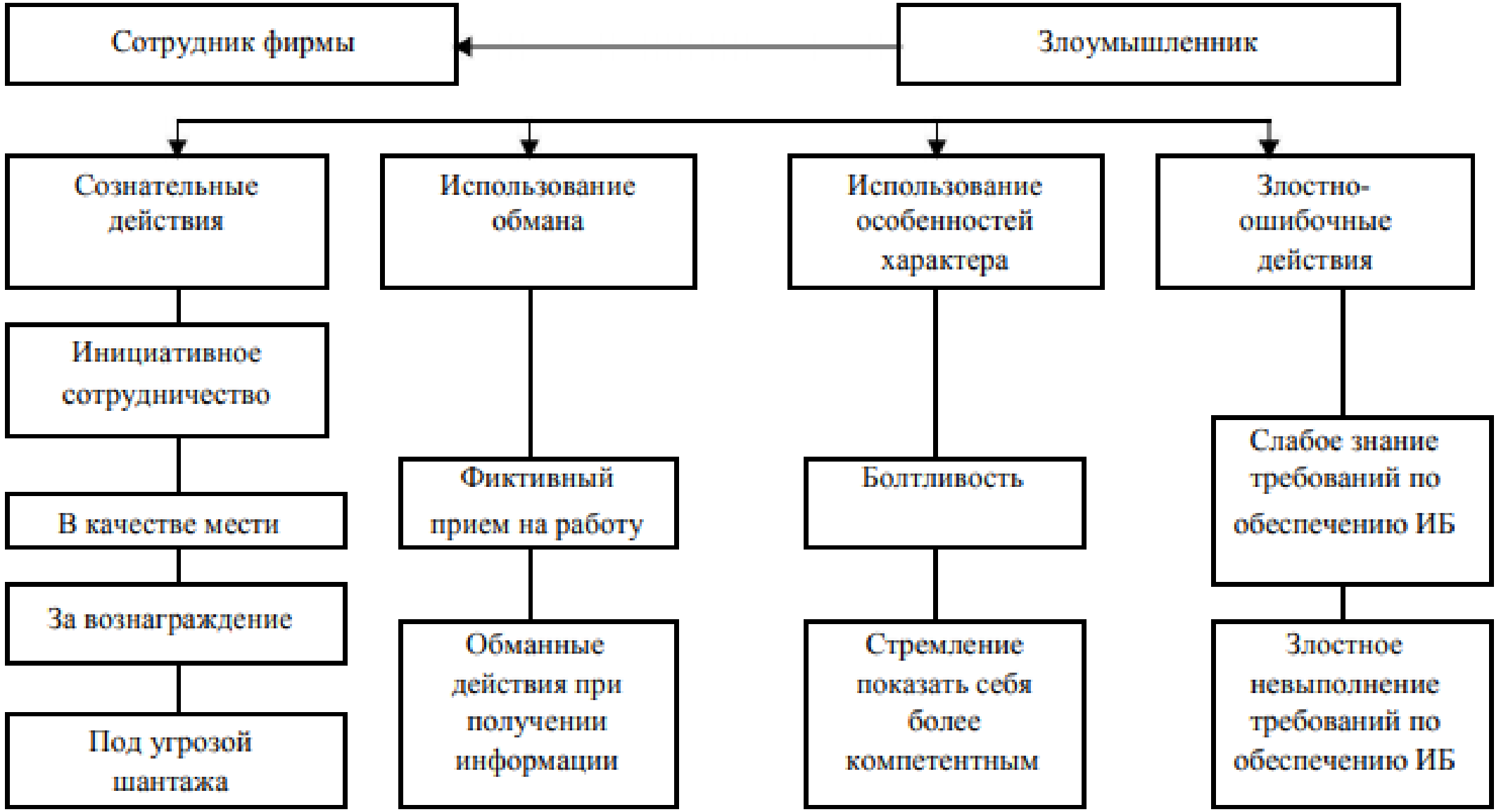
Бесконтрольный выход КИ за пределы организации или круга лиц, которым она была доверена

Возможна по каналам:
– визуально-оптическим;
– акустическим;
– электромагнитным;
– материально-вещественным

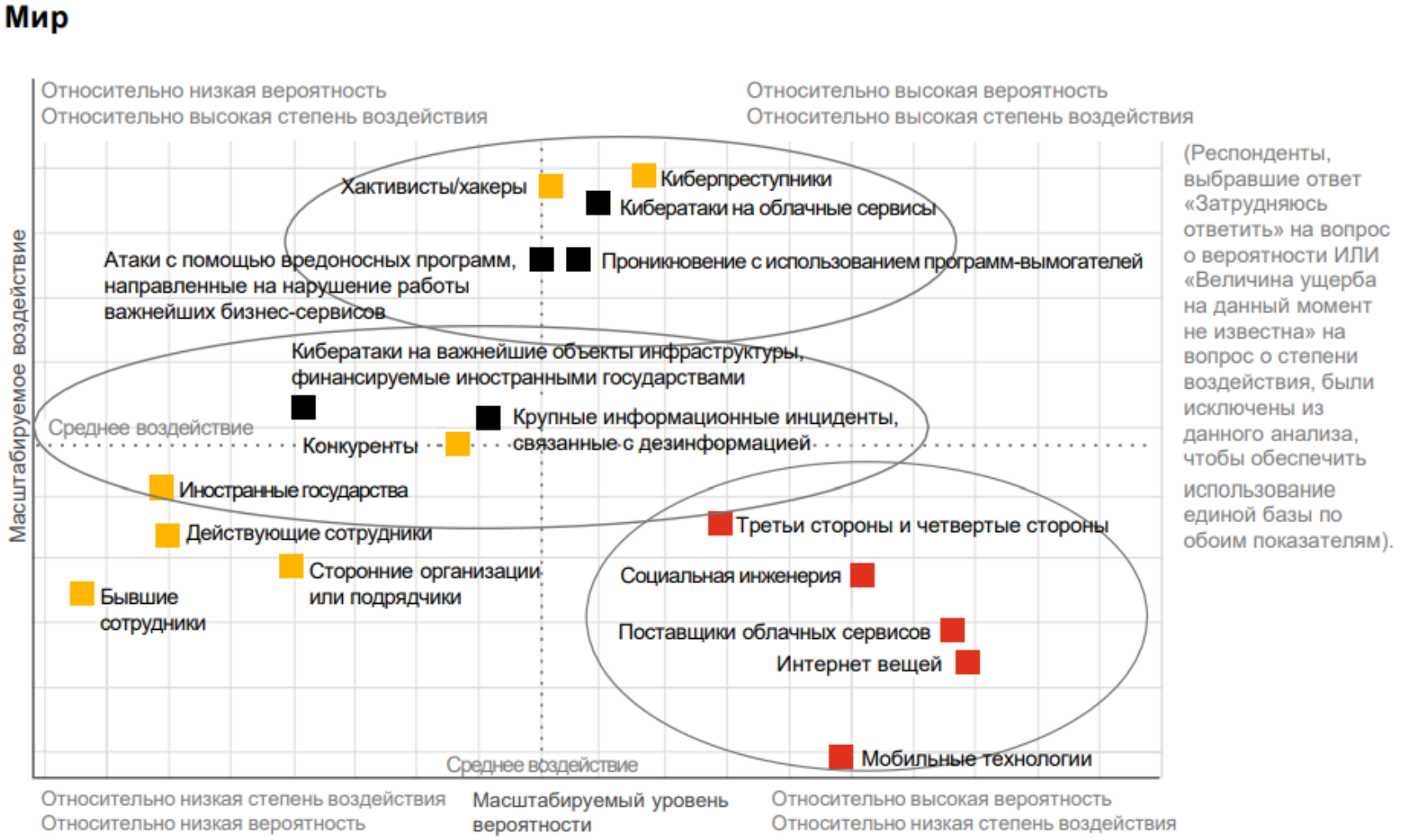
Противоправное преднамеренное ознакомление с КИ недопущенных лиц. Нарушение целостности и доступа к защищаемой информации

Реализуется способами:
– сотрудничество;
– склонение к сотрудничеству;
– выведывание;
– подслушивание;
– наблюдение;
– хищение;
– копирование;
– подделка;
– уничтожение;
– подключение;
– перехват;
– негласное ознакомление;
– фотографирование;
– сбор и аналитическая обработка

Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности

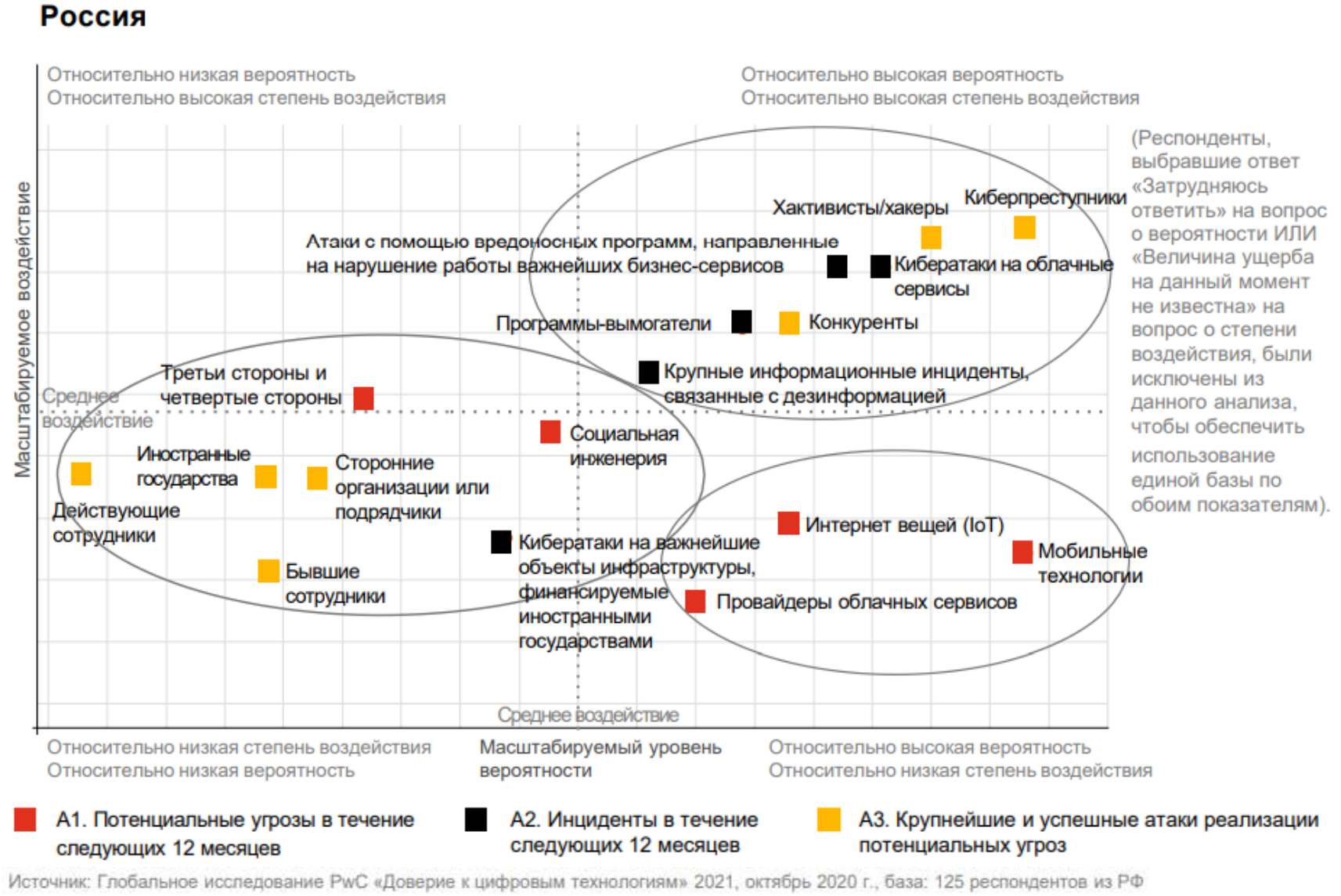


Угрозы, исполнители и события: относительная вероятность и воздействие



Источник: Глобальное исследование PwC «Доверие к цифровым технологиям» 2021, октябрь 2020 г., база: 3 217 респондентов

Угрозы, исполнители и события: относительная вероятность и воздействие



Источник: Глобальное исследование PwC «Доверие к цифровым технологиям» 2021, октябрь 2020 г., база: 125 респондентов из РФ

9. Типовые модели нарушителя для различных категорий лиц

Нарушитель информационной безопасности

- **Нарушитель информационной безопасности** – физическое лицо, случайно или преднамеренно совершающий действия, следствием которых является нарушение информационной безопасности (конфиденциальности, целостности или доступности информации).

- Другими словами, **нарушитель** – это лицо, осуществляющее попытку выполнения запрещенных операций с данными.

- **Злоумышленником** называют нарушителя, который предпринимает такую попытку намеренно и, как правило, из корыстного интереса

Типовые модели нарушителя для различных категорий лиц

Категория	**Тип нарушителя**	Характеристика	Физподготовка	Знания о возможностях технических средств охраны (ТСО)	Оснащённость	Примечание
1	**Профессионал**	Очень опасен. Способен добывать сведения об инженерно-технических средствах охраны инженерно-технических средствах охраны (ИТСО), планировать и готовить вторжение. Действует в одиночку, как правило, не интересуется материальными ресурсами. Опасается огласки	Отличная	Высокие	Специальный набор средств, предназначенный для несанкционированного доступа (НСД), недоступен к свободному приобретению	Тренируется государством и используется в его интересах. Защита от его проникновения - безнадёжное дело, это по силам государственным структурам
2	**Наёмник (любитель)**	Опасен. Способен на нелогичные действия, имеет зачатки плановости действий, может собирать сведения об ИТСО. Действует как в одиночку, так и группой. Интересует весь спектр целей вторжения	Достаточная	Хорошие	Подобранный под задачу НСД набор доступных, но усовершенствованных или самодельных средств	Его услуги стоят дорого - цель его НСД на предприятие должна оправдывать затраты на его наём

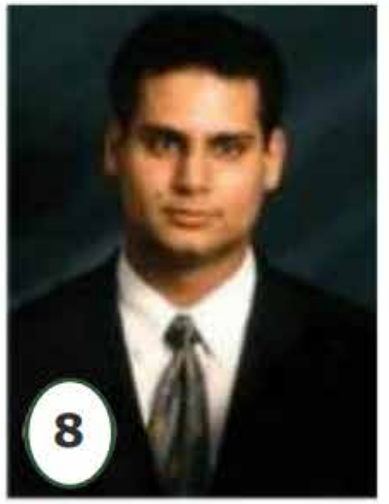
Типовые модели нарушителя для различных категорий лиц

Категория	**Тип нарушителя**	Характеристика	Физподготовка	Знания о возможностях ТСО	Оснащённость	Примечание
3	**Безработный (дилетант)**	Умеренно опасен. Вторжение планируется на дилетанском уровне по сценарию героев популярных фильмов. Действует, как правило, в одиночку. Интересуют либо материальные, либо информационные ресурсы	Удовлетворительная	Слабые	Бытовые средства, легко доступные для приобретения в магазине	Остро нуждающийся в средствах - услуги его дёшевы. Может преследовать свои цели по обогащению
4	**Бытовой (хулиган, наркоман, алкоголик)**	Слабо опасен. Действует импульсивно, на основании обрывочных данных о возможной наживе. Действует как в одиночку, так и группой. Интересуют главным образом материальные (финансовые) ценности. Рассчитывает на силовые приёмы	Плохая	Отсутствуют	Подручные средства (что под руку попалось)	Совершает НСД из хулиганских целей либо в целях обогащения. Услуги его очень дёшевы

Типовые модели нарушителя для различных категорий лиц

Категория	**Тип нарушителя**	Характеристика	Физподготовка	Знания о возможностях ТСО	Оснащённость	Примечание
5	**Сотрудник предприятия**	Опасен. Способен добывать сведения об ИТСО, планировать и готовить НСД, произвести саботаж ТСО. Действует скрытно, в рабочее время, как в одиночку, так и группой. Интересуют либо материальные, либо информационные ресурсы, но малых размеров, позволяющих их пронос (провоз) через КПП. Может привлекать внешних пособников	Плохая	Высокие	Подобранный под задачу НСД набор доступных, но усовершенствованных или самодельных средств	Остро нуждающийся в средствах. Его услуги стоят дорого - цель его НСД на предприятие должна оправдывать затраты на его наём и потерю работы. Либо преследует свои цели по обогащению

Кибер-преступник, кто он? Как узнать? Попробуйте идентифицировать



Кибер-преступник, кто он? Как узнать? Наши герои:

- **1. Фрэнк Абигнейл** - был приговорен к 12 годам лишения свободы за мошенничество.
- **2. Ванг Женгянг** - 13 лет. Взломал компьютерную систему школы с целью прогуливать уроки. Он также обвинялся в мошенничестве при оплате товара в онлайн магазине, где он изменил стоимость ноутбука с $400 на $0,16.
- **3. Оуен Вокер** - обвинялся в организации международной преступной хакерской группы, во взломе систем, создании бот-сетей. Был освобожден от заключения, так как не достиг совершеннолетия.
- **4. Кевин Митник** - неоднократно совершал преступления, связанные с проникновением в компьютерные сети.
- **5. Дэвид Кернелл** - предъявлено обвинение во взломе электронной почты американского политика Сары Палин.
- **6. Джозеф МакЭлрой** - приговорен к 200 часам общественных работ за проникновение в сеть государственного учреждения США. На момент проникновения ему было 16 лет.
- **7. Кристина Шечинская** - 21 летняя россиянка. Одна из девяти соучастников обвиняемых в хищении 3 миллионов долларов из американских банков при помощи хакерского ПО
- **8. Саад Ичуафни** - разыскивается ФБР за организацию и проведение DDOS - атак.

Нарушители

- Чтобы построить качественную модель угроз, **необходимо иметь представление о возможных нарушителях информационной безопасности**, поскольку искусственные угрозы (особенно преднамеренные) являются наиболее опасными.
- Для этого предварительно **создается модель нарушителя** информационной безопасности.
- Она состоит из профилей (описаний) вероятных нарушителей, каждый из которых включает следующие предположения:
  - 1. Категория лиц, к которым может принадлежать нарушитель
  - 2. Мотивы нарушителя
  - 3. Уровень знаний нарушителя (в контексте анализируемой системы)
  - 4. Возможности нарушителя (используемые методы и средства)
  - 5. Время действия
  - 6. Место действия

Нарушители

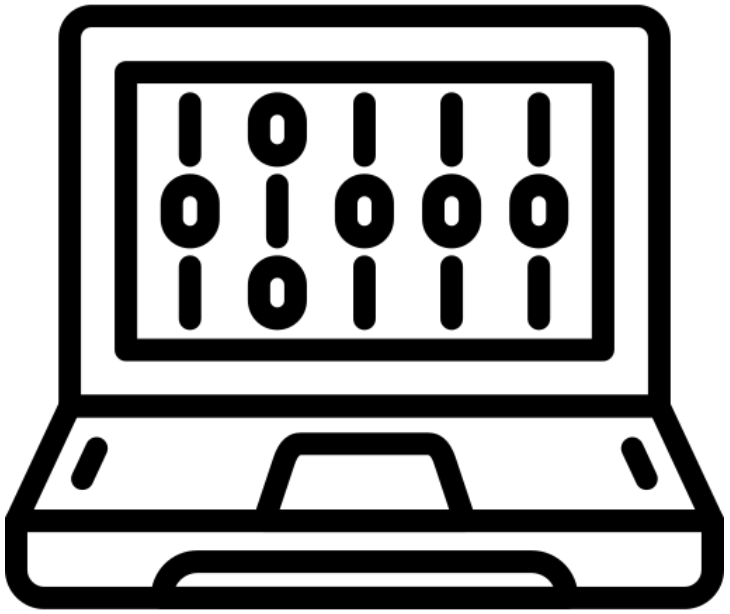
- **1. Категория лиц, к которым может принадлежать нарушитель.**
  - **Внешние нарушители**. Бывшие сотрудники предприятия, клиенты, посетители, конкуренты, случайные лица, преступные группировки.
  - **Внутренние нарушители (инсайдеры).** Более опасная категория. Включает пользователей системы, обслуживающий персонал, разработчиков АИС, сотрудников службы безопасности, руководителей и т. д.
- **2. Мотивы нарушителя:**
  - **безответственность** (нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла);
  - **самоутверждение** (получая доступ к запретным данным, нарушитель растет в своих глазах или глазах коллег; свои действия часто воспринимает как игру);
  - **корыстный интерес**.

Нарушители

- **3. Уровень знаний нарушителя (в контексте анализируемой системы):**
  - пользователь;
  - администратор;
  - программист;
  - специалист в области информационной безопасности.
- **4. Возможности нарушителя (используемые методы и средства):**
  - может получать сведения только от других лиц;
  - использует штатные средства доступа к данным (возможно, в несанкционированном режиме);
  - пассивный перехват;
  - активный перехват (возможность модификации данных).

Нарушители

- **5. Время действия:**
  - во время функционирования информационной системы;
  - во время простоя системы;
  - в любое время.
- **6. Место действия:**
  - без доступа на контролируемую территорию организации;
  - с доступом на контролируемую территорию (но без доступа к техническим средствам);
  - с рабочих мест пользователей;
  - с доступом к базам данных АИС;
  - с доступом к подсистеме защиты АИС.

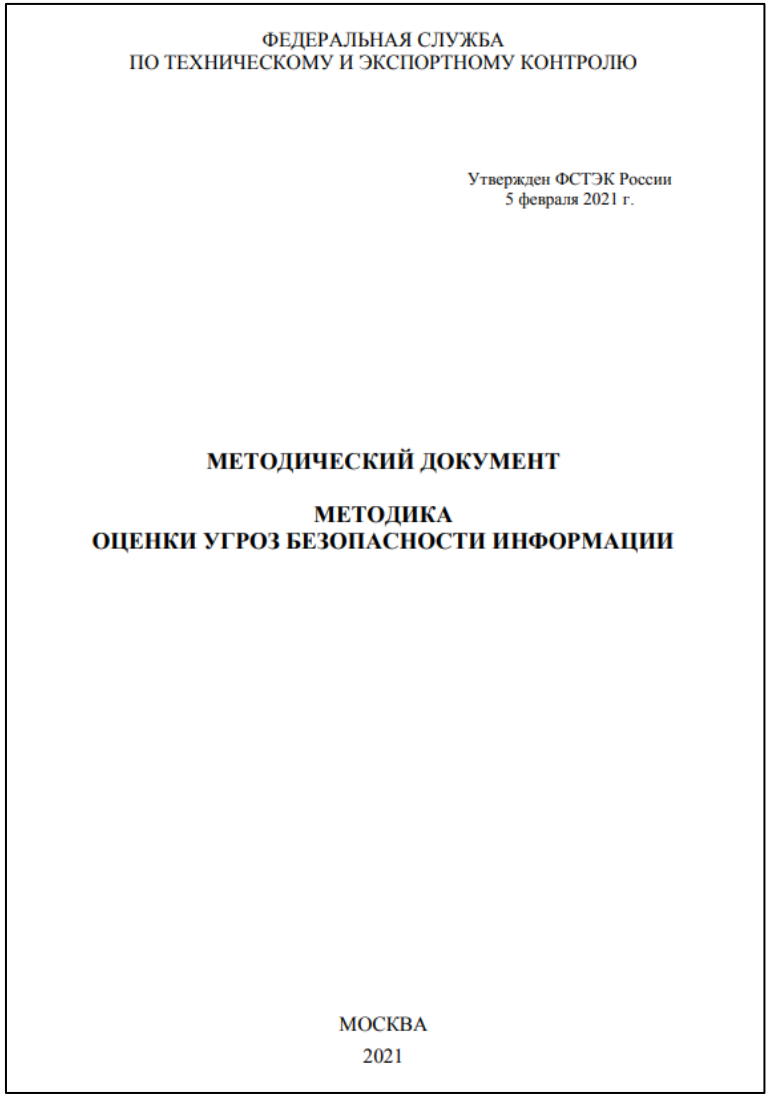


10. Методики оценки и моделирования угроз

10.1 Методика оценки угроз безопасности информации ФСТЭК России

Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.
https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021#

Методика оценки угроз безопасности информации



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021

- **Методика оценки угроз безопасности информации.** Методический документ. Утвержден Федеральной службой по техническому и экспортному контролю (ФСТЭК) России 5 февраля 2021 г.

- https://fstec.ru/component/attachments/download/2919
- https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021#

Методика оценки угроз безопасности информации

- **Методика определяет порядок и содержание работ по определению угроз безопасности информации**, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах), а также по разработке моделей угроз безопасности информации систем и сетей.

https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

Оценка угроз безопасности информации

- **Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации**, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.

Задачи решаемые в ходе оценки угроз информационной безопасности

- **Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются**:
  - **а) определение негативных последствий**, которые могут наступить от реализации (возникновения) угроз безопасности информации;
  - **б) инвентаризация систем и сетей** и определение возможных объектов воздействия угроз безопасности информации;
  - **в) определение источников угроз** безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
  - **г) оценка способов реализации** (возникновения) угроз безопасности информации;
  - **д) оценка возможности реализации** (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
  - **е) оценка сценариев реализации угроз** безопасности информации в системах и сетях.

Исходные данные для оценки угроз

- **Исходными данными для оценки угроз безопасности информации являются:**
- **а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России** (http://bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

Исходные данные для оценки угроз

- **Исходными данными для оценки угроз безопасности информации являются:**
- **б)** описания векторов **(шаблоны) компьютерных атак**, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет»
  - **CAPEC,**
  - **ATT&CK,**
  - **OWASP,**
  - **STIX,**
  - **WASC**
  - и др.;

Исходные данные для оценки угроз

- **Исходными данными для оценки угроз безопасности информации являются:**
- **в) документация на системы и сети** (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);
- **г) договоры, соглашения или иные документы**, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

Исходные данные для оценки угроз

- **Исходными данными для оценки угроз безопасности информации являются:**
- **д) нормативные правовые акты Российской Федерации**, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- **е) технологические, производственные карты** или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее – основные (критические) процессы);
- **ж) результаты оценки рисков** (ущерба), проведенной обладателем информации и (или) оператором.
- Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют системы и сети.

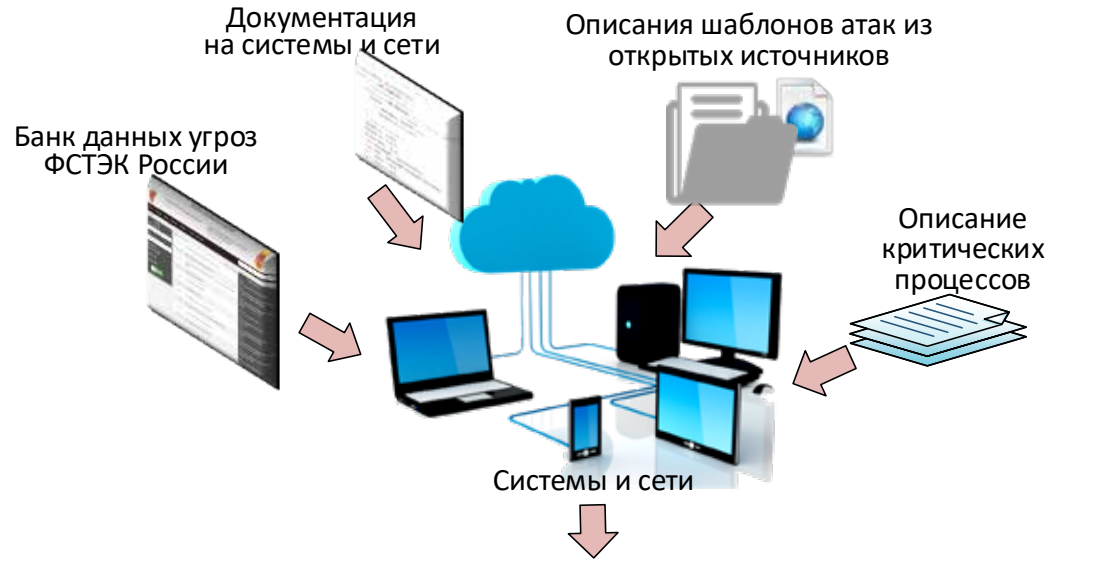
Оценка угроз безопасности информации должна носить систематический характер

- **Оценка угроз безопасности информации должна носить систематический характер** и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей.
- Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей.
- Учет изменений угроз безопасности информации обеспечит своевременную выработку адекватных и эффективных мер по защите информации (обеспечению безопасности) в системах и сетях.

Результаты оценки

- **По результатам оценки должны быть выявлены актуальные угрозы безопасности информации**, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей.

Общая схема проведения оценки угроз безопасности информации



Этап 1. Определение негативных последствий

- Анализ документации систем и сетей и иных исходных данных
- Определение негативных последствий от реализации угроз

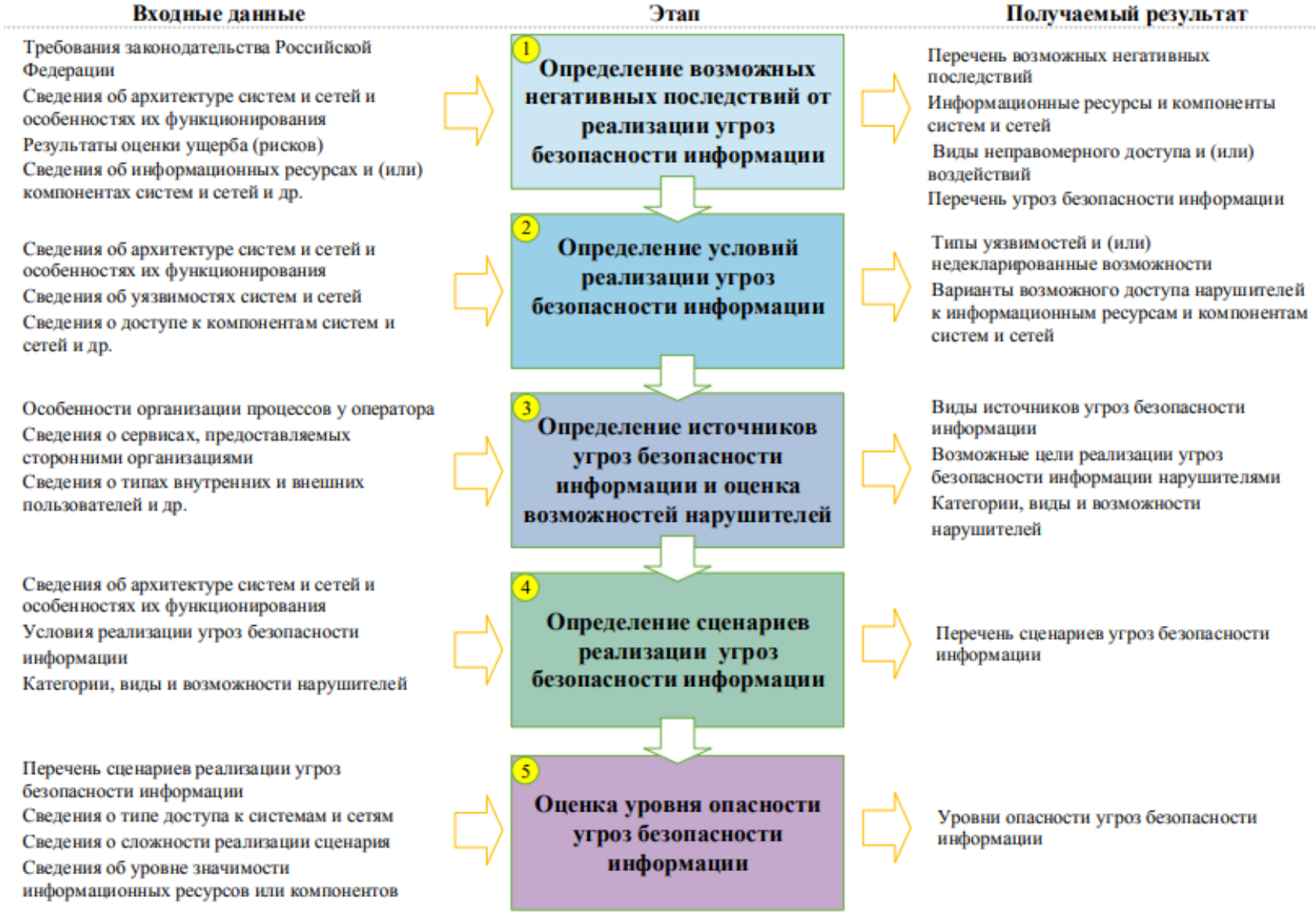
Этап 2. Определение объектов воздействий

- Анализ документации систем и сетей и иных исходных данных
- Инвентаризация систем и сетей
- Определение групп информационных ресурсов и компонентов систем и сетей

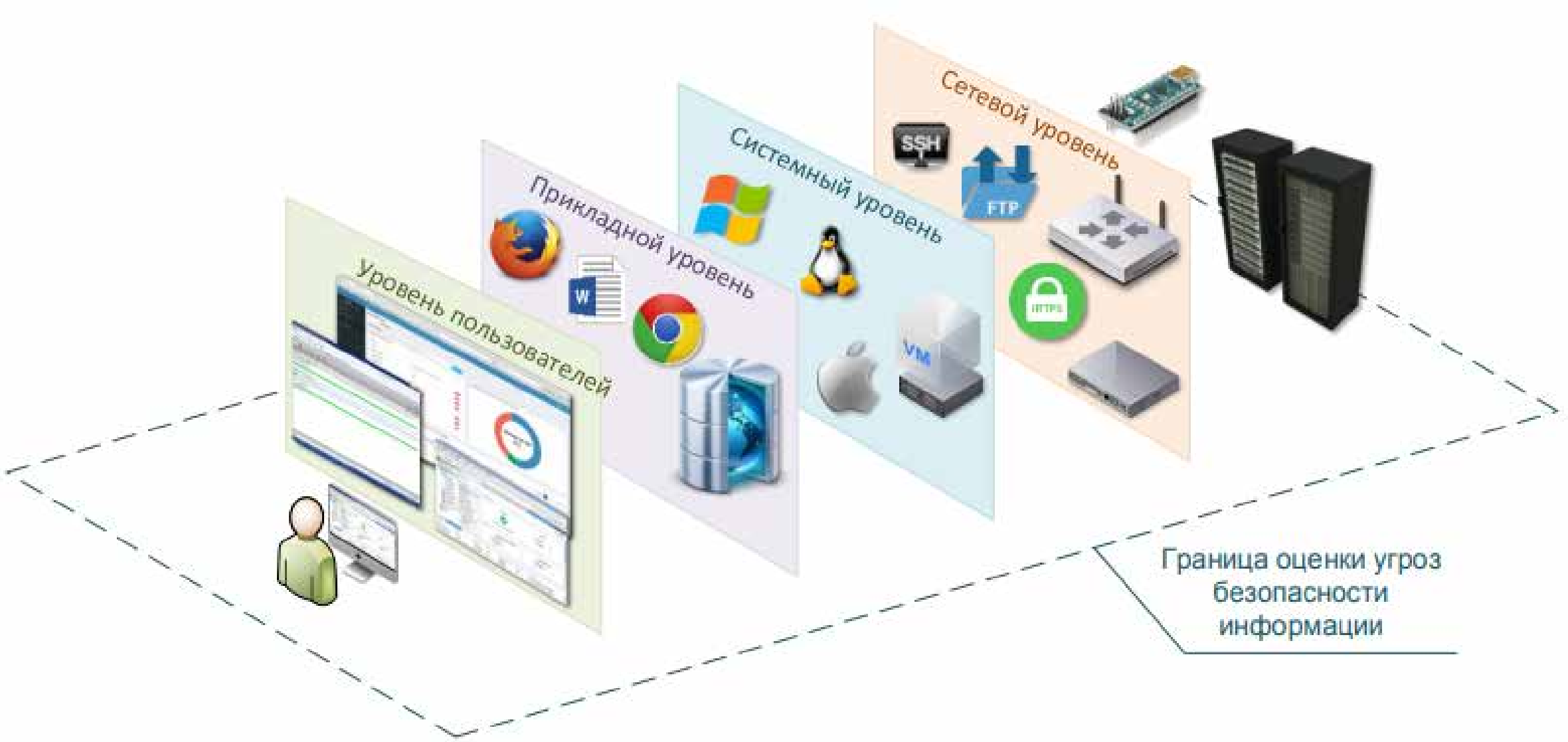
Этап 3. Оценка возможности реализации угроз и их актуальности

- Определение источников угроз
- Оценка способов реализации угроз
- Оценка актуальности угроз

Порядок моделирования угроз безопасности

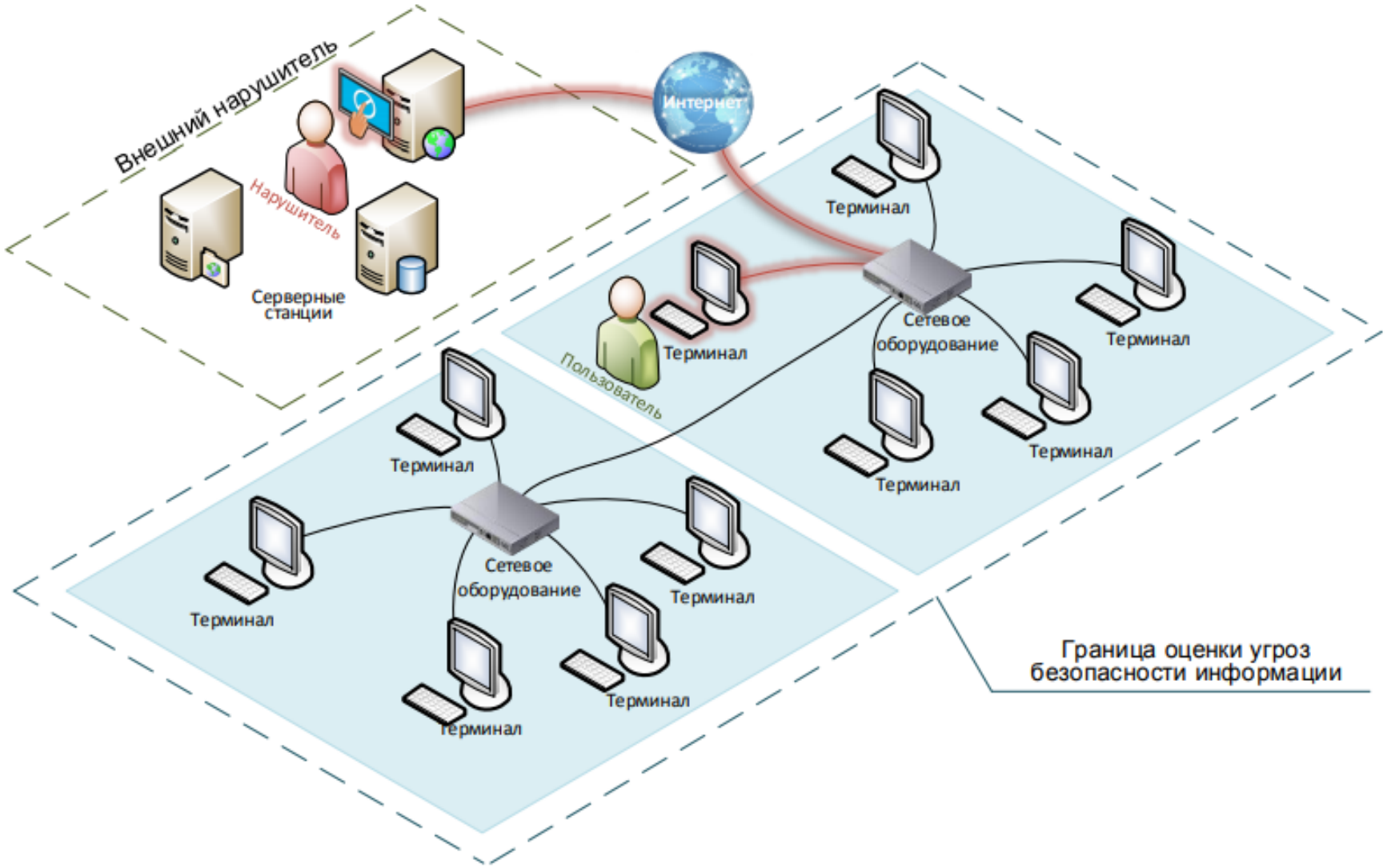


Уровни архитектуры систем и сетей, на которых определяются объекты воздействия

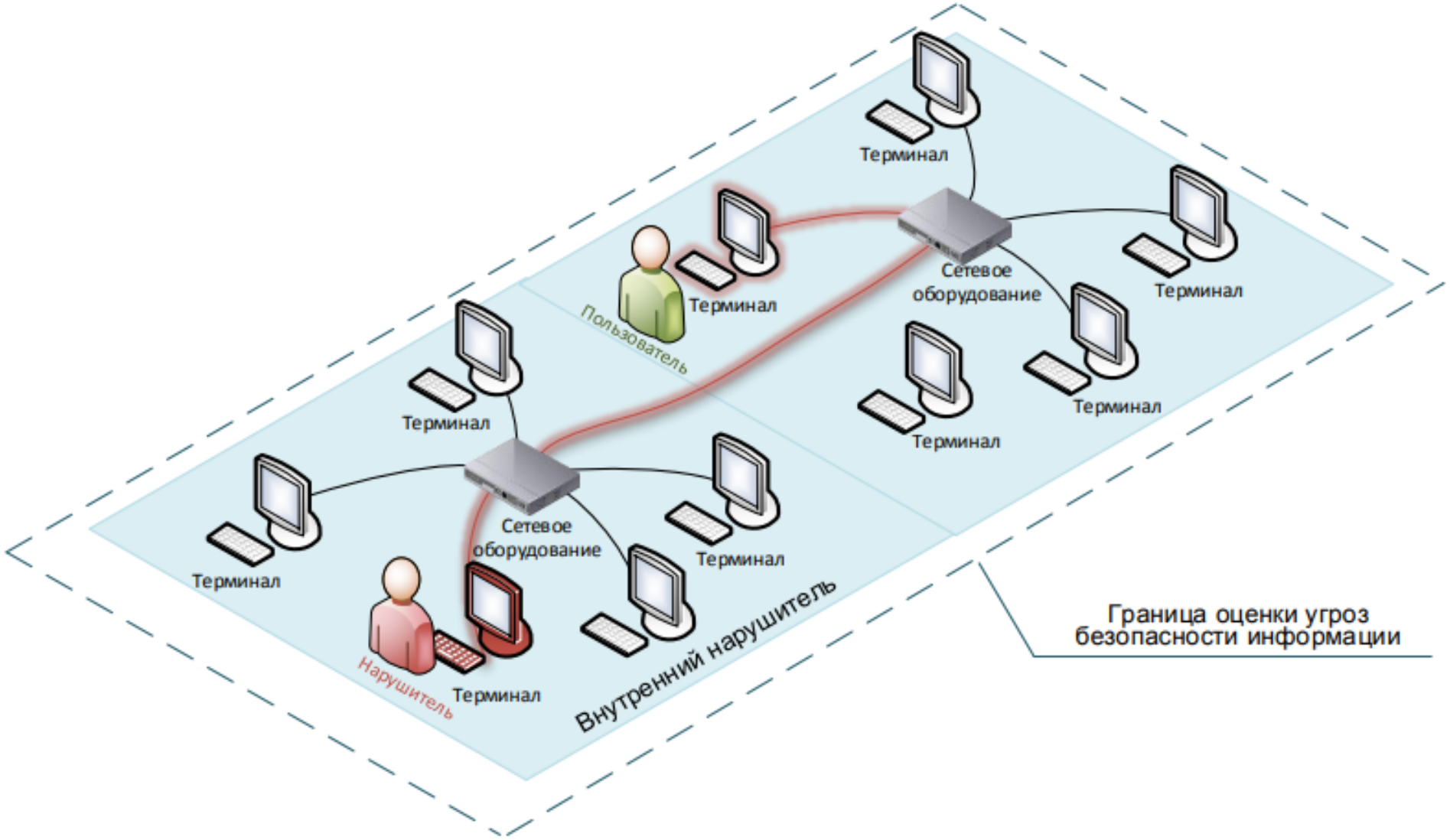


Пример распределения границ при оценке угроз безопасности информации в информационной инфраструктуре поставщика услуг

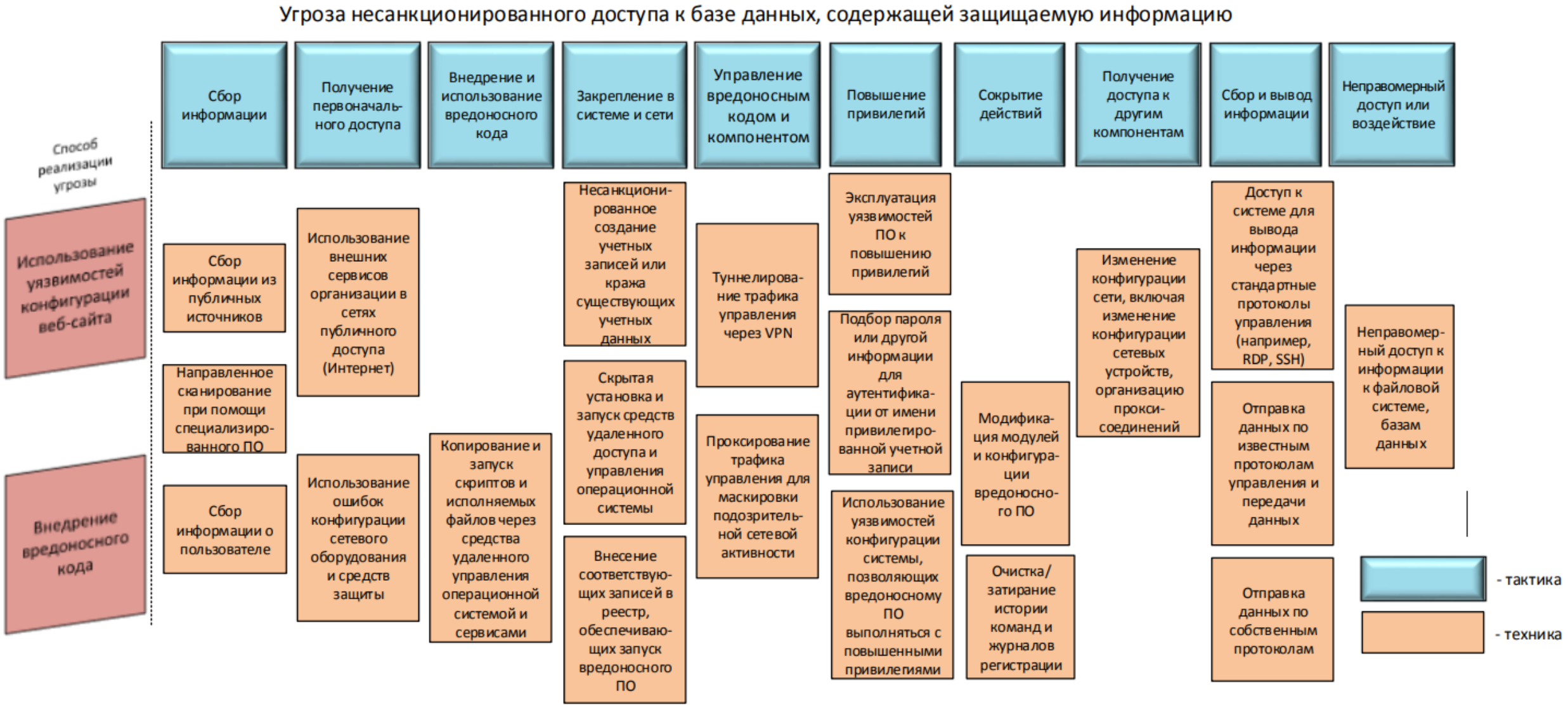
Внешний нарушитель при реализации угроз безопасности информации



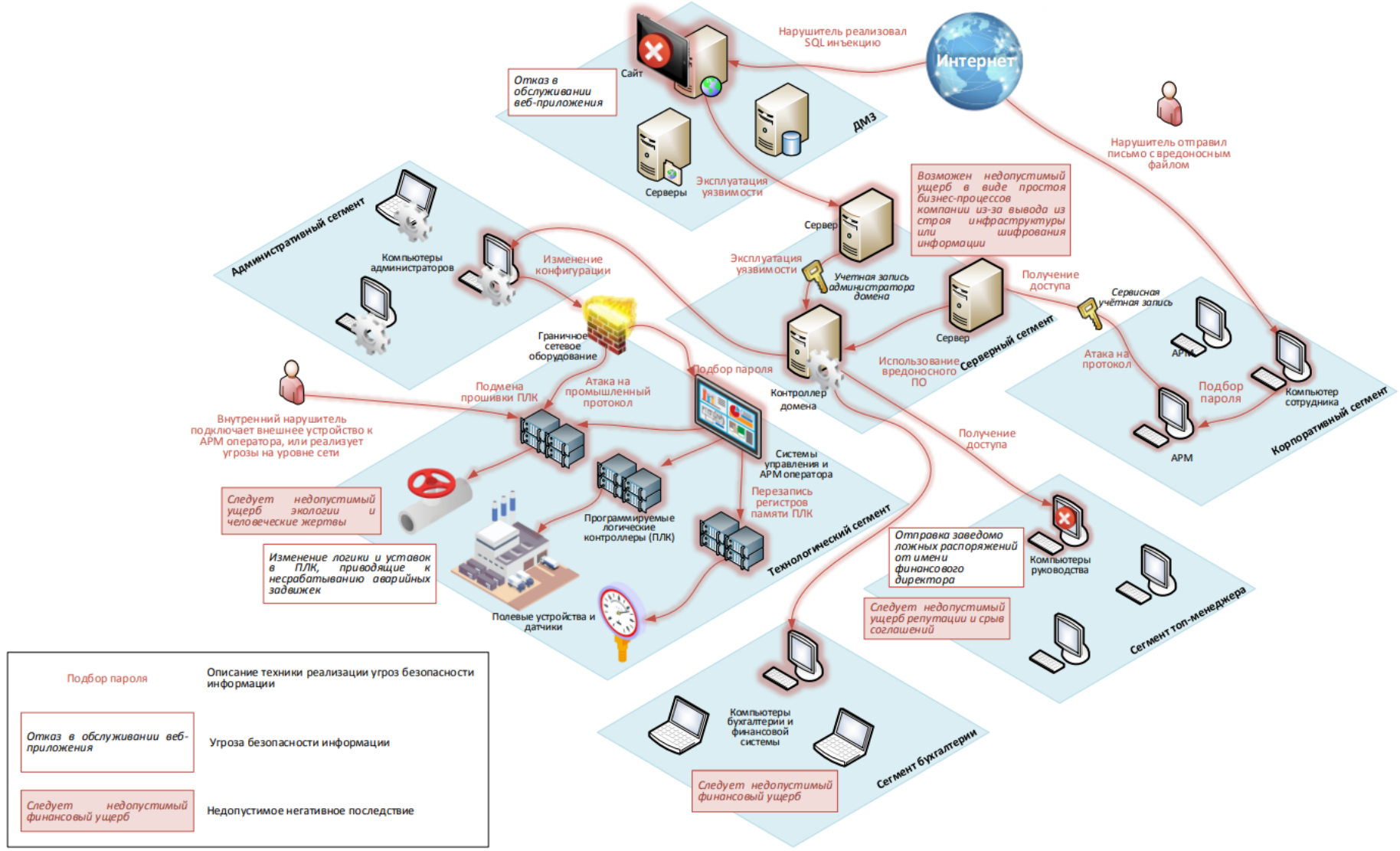
Внутренний нарушитель при реализации угроз безопасности информации



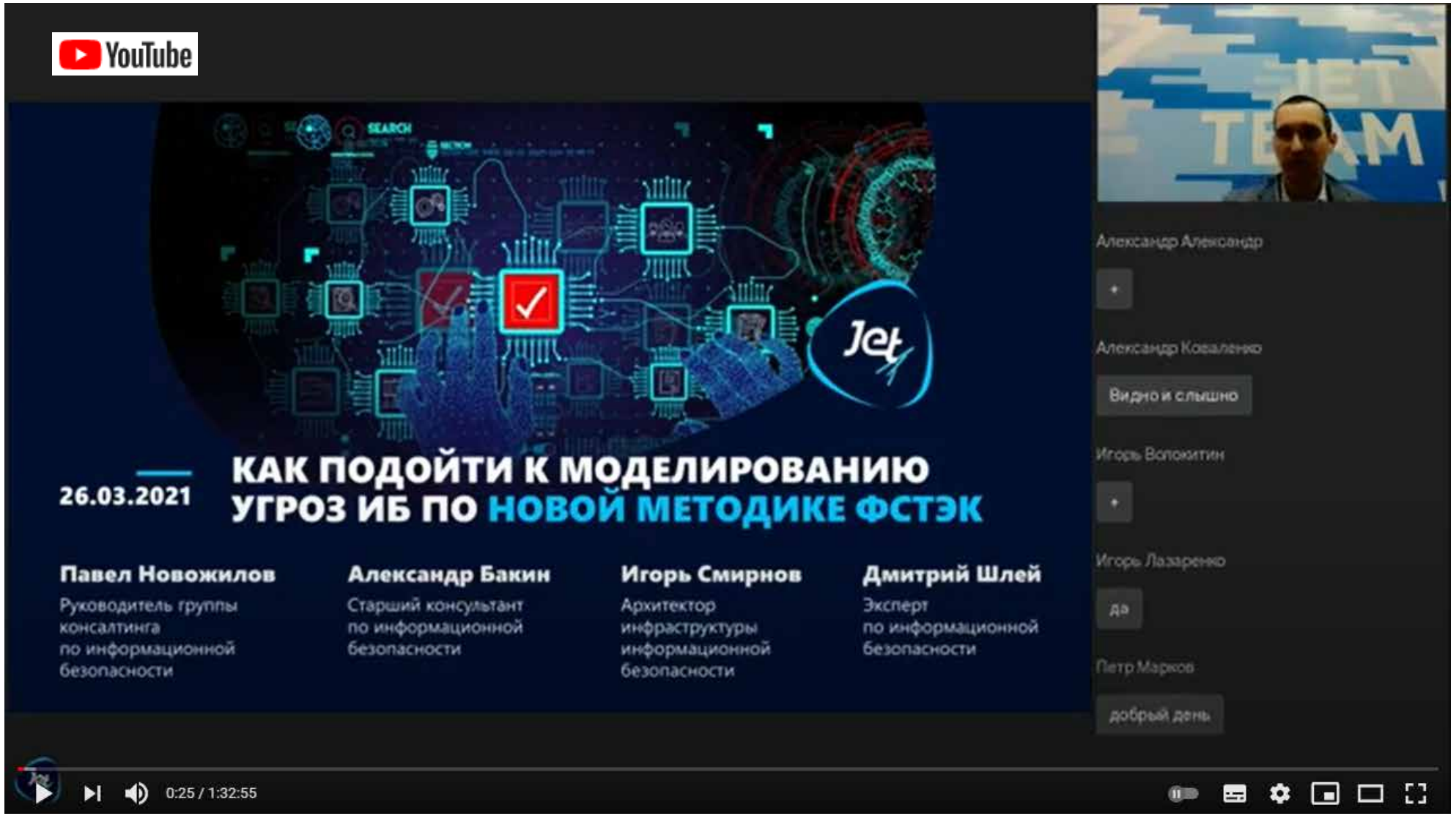
Пример сценария реализации угрозы безопасности информации



Пример сценариев реализации угроз безопасности информации

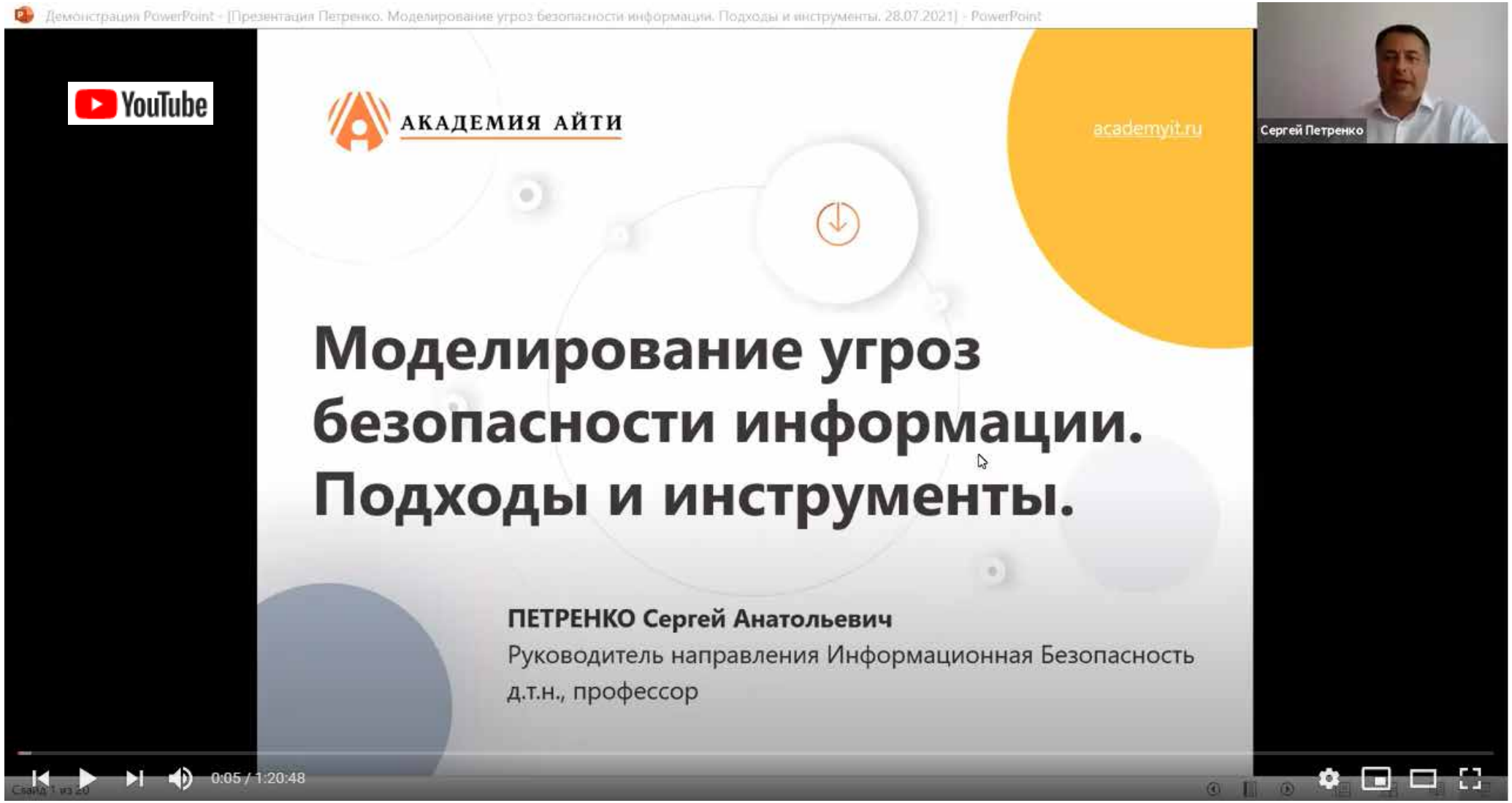


Дополнительные материалы



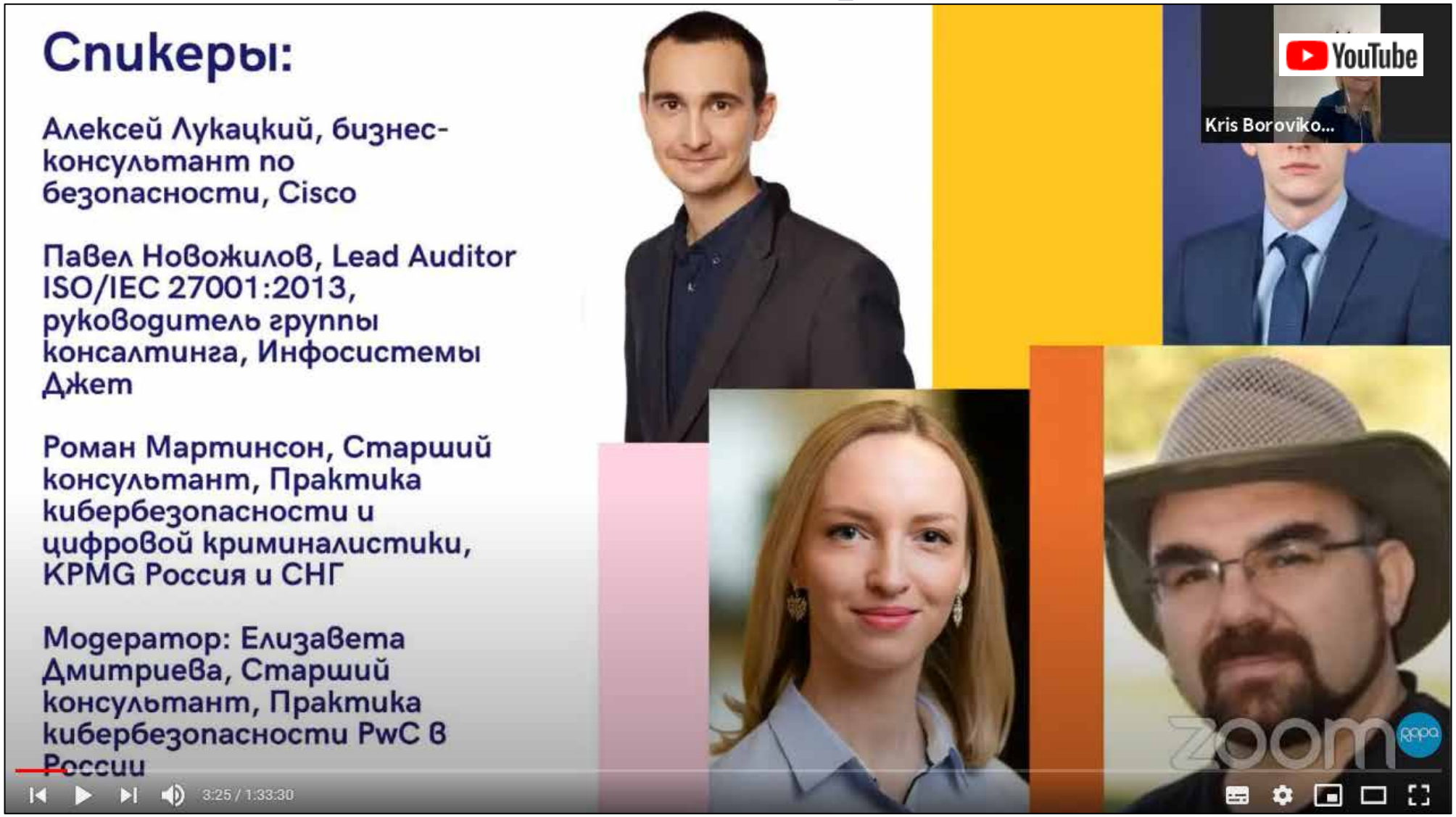
Новая методика ФСТЭК. Как теперь моделировать угрозы ИБ? (апрель 2021)
https://www.youtube.com/watch?v=rzDAJS0QVww

Дополнительные материалы



Моделирование угроз безопасности информации Подходы и инструменты
https://www.youtube.com/watch?v=CChVkqJ7p-I&list=PLQfolpjf5pQKHtNhnq-_yxFWiJLB0uRQn&index=1

Дополнительные материалы

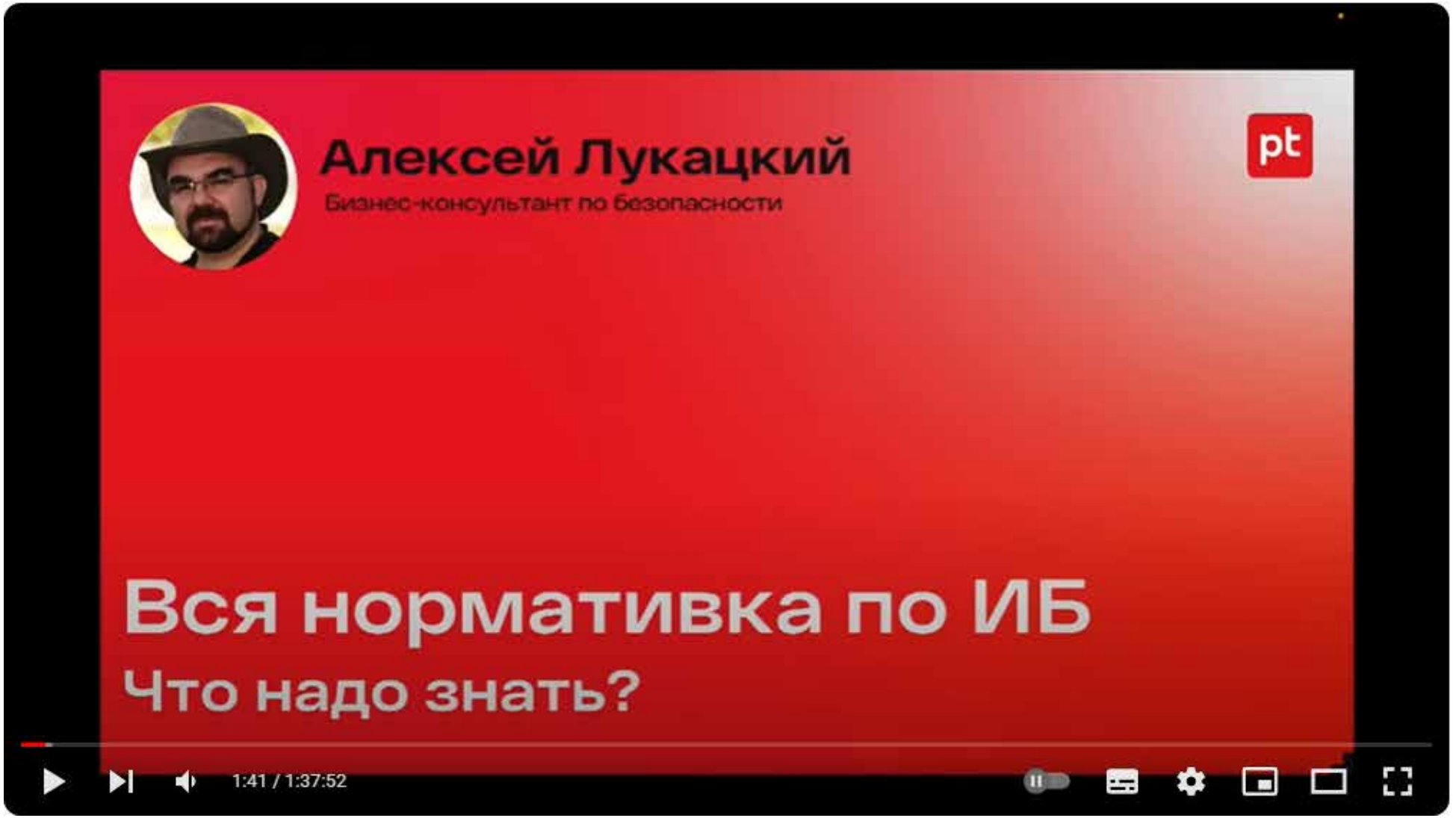


Семинар RPPA - Методика оценки угроз безопасности информации ФСТЭК
https://www.youtube.com/watch?v=e02qqjxJwEc&list=PLQfolpjf5pQKHtNhnq-_yxFWiJLB0uRQn&index=3

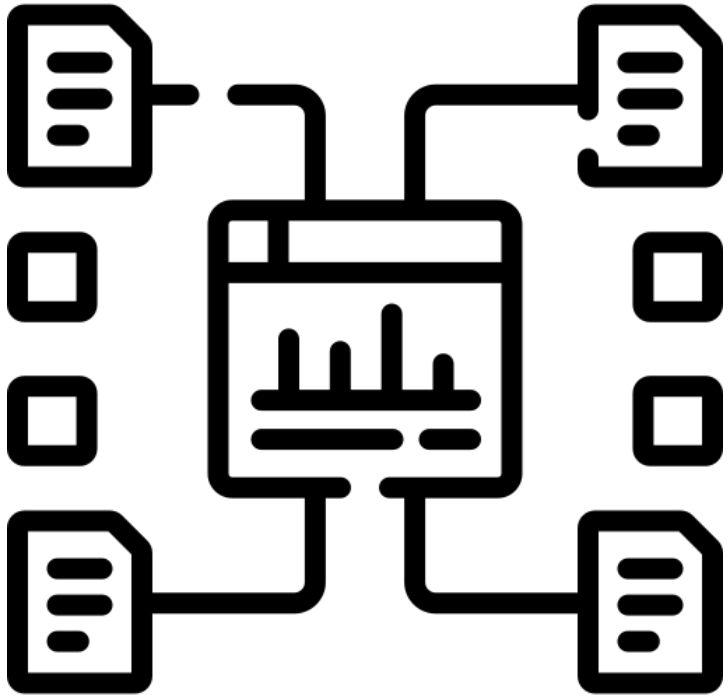
Дополнительные материалы

Алексей Лукацкий. Основные сценарии реализации угроз и их преломление на методику оценки ФСТЭК
https://www.youtube.com/watch?v=R4a2_k_YVwc

Дополнительные материалы



Законодательные требования РФ по информационной безопасности 2023 | Алексей Лукацкий
https://www.youtube.com/watch?v=qfxj-vHr5lU



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

10.2 Методология моделирования угроз и защитных мер от MITRE

Threat Assessment and Remediation Analysis (TARA)

MITRE

- **MITRE** — это некоммерческая организация, которая работает в США и управляет центрами исследований и разработок на уровне федерального правительства и местного самоуправления.

- В зону интересов MITRE входят:
  - искусственный интеллект,
  - квантовая информатика,
  - информатика в области здравоохранения,
  - космическая безопасность,
  - обмен данными о киберугрозах и средствах защиты
  - и так далее.

Проекты MITRE

- **Список уязвимостей CVE (Common Vulnerabilities and Exposures)** http://cve.mitre.org
- **ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)**, attack.mitre.org — это структурированный список известных техник, приемов и тактик злоумышленников, представленный в виде таблиц;
- **Structured Threat Information Expression (STIX)** — это язык и формат сериализации, используемый для обмена информацией о киберугрозах (CTI — Cyber Threat Intelligence) между системами информационной безопасности;
- **CAR (Cyber Analytics Repository)** — база знаний, разработанная на основе модели ATT&CK. Она может быть представлена в виде псевдокода, и команды защитников могут использовать ее при создании логики детектирования в системах защиты;
- **SHIELD Active Defense** — база знаний по активной защите, которая систематизирует методы безопасности и дополняет меры снижения рисков, представленные в ATT&CK;
- **AEP (ATT&CK Emulation Plans)** — это способы моделирования поведения злоумышленника на основе определенного набора TTP (Tactics, Techniques, and Procedures) по ATT&CK.

Threat Assessment and Remediation Analysis (TARA)

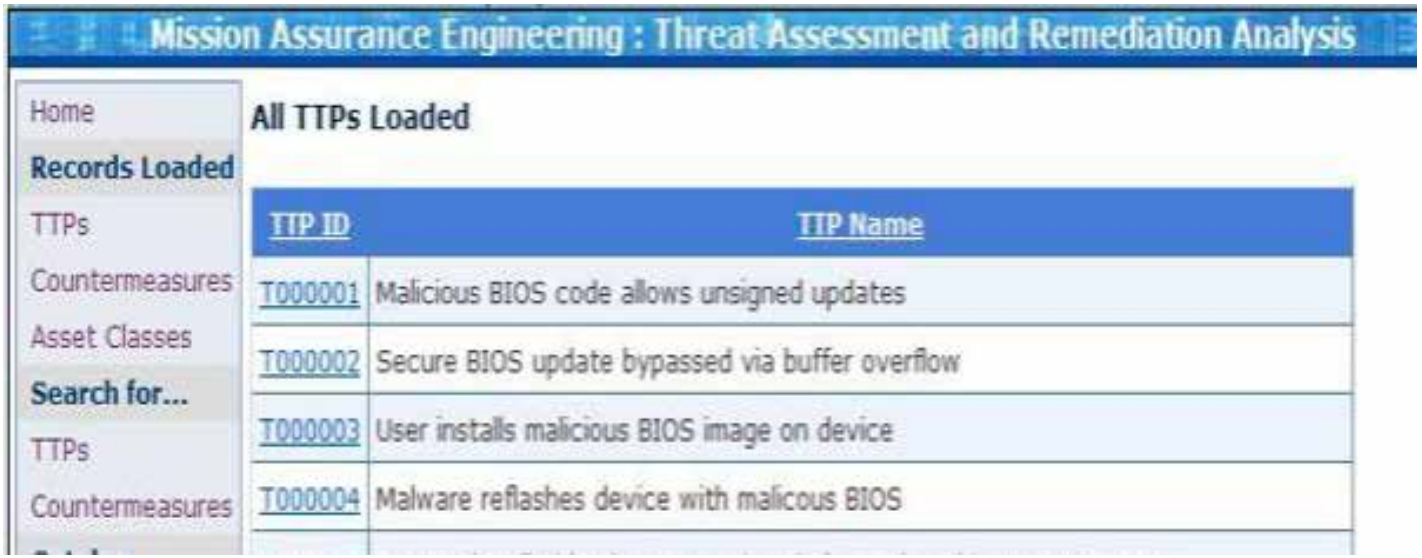
- **Методология TARA включает в себя три активности**
  - анализ угроз (Cyber Threat Susceptibility Analysis),
  - анализ защитных мер (Cyber Risk Remediation Analysis)
  - и разработку данных и инструментов.

- Идеологически, методология TARA очень сильно похожа на то, что описано в методике оценки угроз ФСТЭК, но есть ряд нюансов, которые и отличают эти два подхода; причем существенно.

Threat Assessment and Remediation Analysis (TARA)
https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara
https://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-and-remediation-analysis.pdf

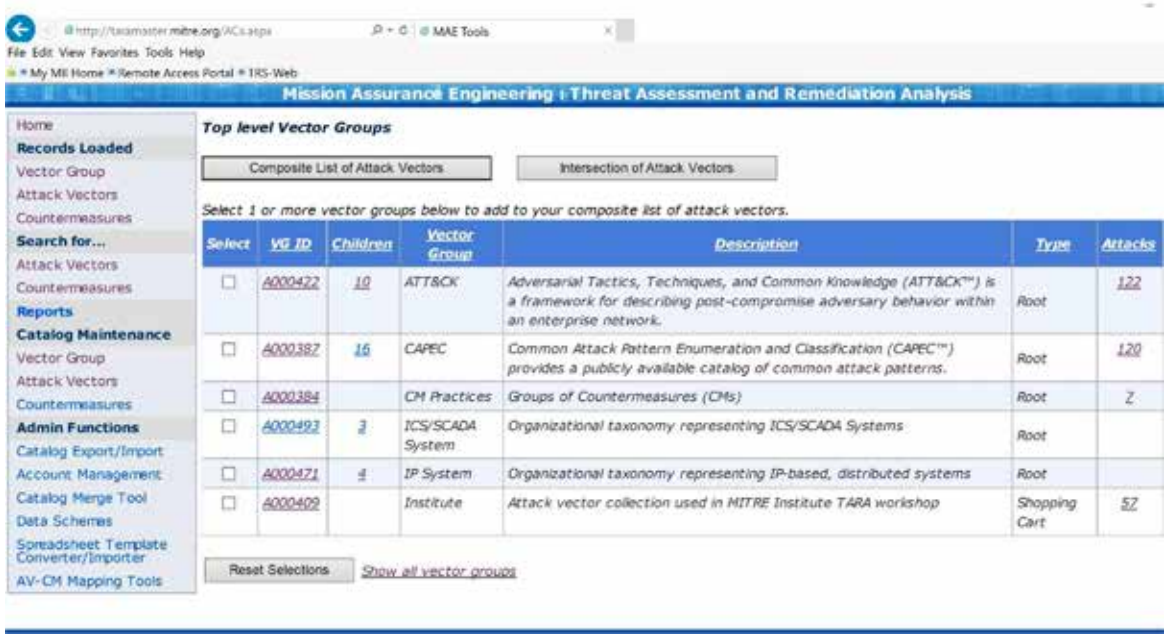
Threat Assessment and Remediation Analysis (TARA)

- **1) Методика не является обязательной к применению**. Право ее выбора лежит на потребителе.
- **2) TARA не ссылается на матрицу техник и тактик MITRE ATT&CK** (ее еще тогда просто не было), но само понятие TTP в методике TARA присутствует ровно в том же контексте, что и в ATT&CK. В последующих версиях TARA это понятие немного трансформировалось в вектора атак, то есть последовательность действий, которые злоумышленник осуществляет для достижения своей цели, но суть опять же не поменялась.



Threat Assessment and Remediation Analysis (TARA)

- **3) Указанные вектора атак объединяются в группы**, которые могут быть классифицированы по разному. Обратите внимание, в конструкторе есть и группа техник MITRE ATT&CK и собственные варианты систематизации векторов атак. Например, у меня может быть группа векторов "аутентификация пользователя по паролю", а вектора, входящие в нее, - атаки по словарю, перебор паролей, радужные таблицы и т.п.



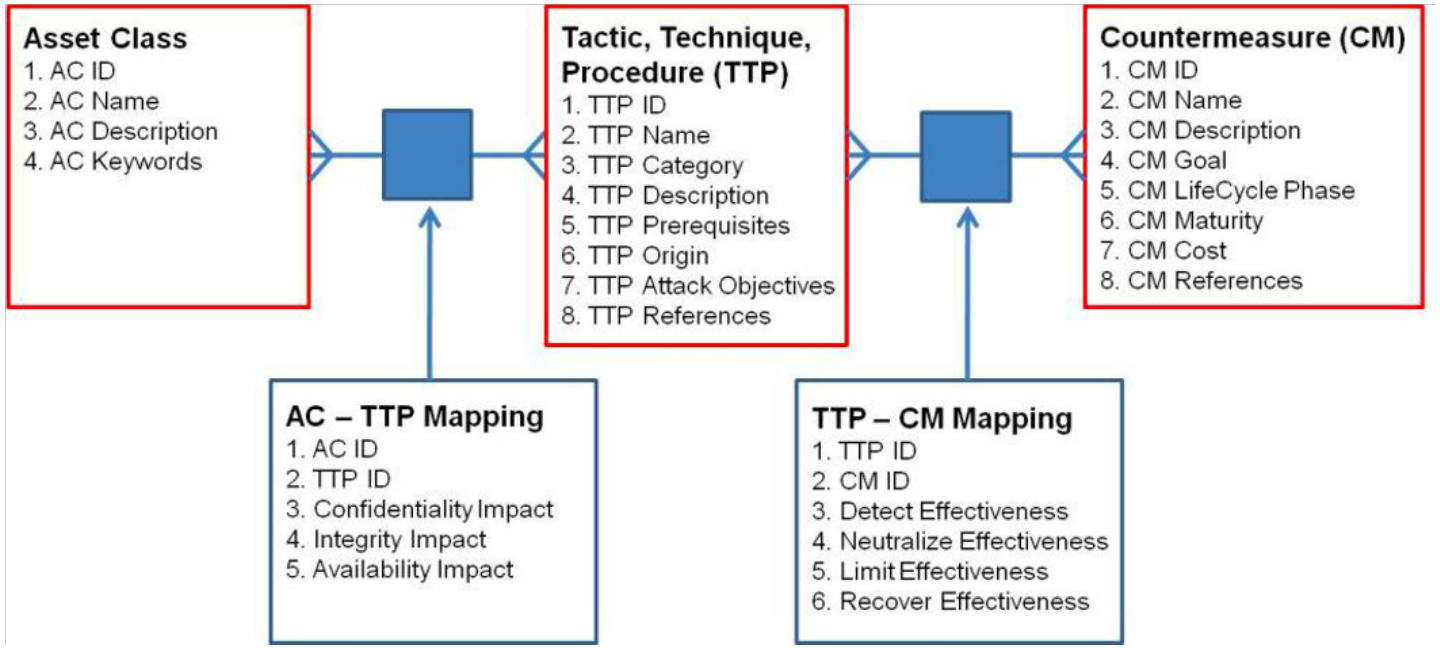
Threat Assessment and Remediation Analysis (TARA)

4) Методика начинается с инвентаризации и оценки защищаемых активов, которая может быть выполнена как самостоятельно, так и с помощью другой методологии MITRE - CJA (Crown Jewels Analysis). При этом TARA не требует описания активов вплоть до интерфейсов и уровней, как это описано у ФСТЭК. Все чуть проще - Web-сервер, браузер, СУБД, приложение e-mail, коммутатор, УПАТС и т.п. Но при необходимости можно и углубиться в детали, если такая задача стоит. Например, сам каталог возможных активов достаточно обширен с точки зрения описываемых атакуемых объектов.

AC ID	AC Name	Keywords
A000223	Applications	antivirus | browser | excel | MS project | MS word | Outlook | pdf reader | powerpoint | visio | vpn | internet explorer | firefox
A000036	authentication	credential | password | account | authentication | certificate | username | authenticate | user | SAML token | credentials
A000187	Data	DOM | html | parse | schema | Unicode | XHTML | XML | cookie | token
A000037	database	database | Oracle | SQL | schema | DBMS | JDBC | MS access | ODBC
A000201	email	email | IMAP | POP | SMTP | Outlook | Thunderbird
A000057	firmware	BIOS | firmware | IOS
A000267	mobile	3G | 4G | 802.11 | access point | cell | cellular | hotspot | mobile | WEP | wi-if | wimax | wireless | WPA
A000098	network service	IDS | IPS | proxy
A000235	OS	android | IOS | linux | OS | unix | windows
A000128	OSI - Application Layer	BGP | DHCP | DNS | FTP | http | HTTPS | IMAP | LDAP | POP | SIP | SMTP | SNMP | SSL
A000140	OSI - Data Link Layer	ARP | OSPF | VLAN
A000136	OSI - Network Layer	ICMP | IP | IPv4 | IPv6
A000131	OSI - Transport Layer	TCP | UDP
A000251	PKI	certificate | CRL | keystore | PKI | revocation | root | self-signed | X.509 | X509 | CA | certificate authority
A000051	platform	bridge | cloud | firewall | gateway | hub | router | server | switch | thick client | thin client | wireless
A000228	Remote access	IPsec | SSH | telnet | vpn
A000179	Scripting	CGI | JavaScript | Perl | PHP | Python | flash | bash
A000172	Security	access matrix | ACL | AES | biometric | certificate | CHAP | DES | digital signature | EAP | encryption | firewall | hash | IPsec | kerberos | L2F | L2TP | MD5 | packet filter | password | PKI | PPTP | radius | security | SHA | SSH |

Threat Assessment and Remediation Analysis (TARA)

5) Методика очень сильно завязана на так называемые каталоги, которые и содержат уже скрупулезно собранные и систематизированные техники и тактики угроз, вектора атак, защитные меры, активы и т.п. Эти каталоги позволяют легко автоматизировать процедуру моделирования угроз. Модель данных этих каталогов выглядит следующим образом:



Threat Assessment and Remediation Analysis (TARA)

6) Наличие в каталогах данных как из открытых, так и закрытых источников. В зависимости от оцениваемого объекта такое деление позволяет использовать более широкий круг источников данных, в том числе и грифованных, для оценки возможных векторов атак и негативных последствий от их использования. Из открытых источников TARA использует CAPEC, CWE, CVE.

Threat Assessment and Remediation Analysis (TARA)

7) Скоринговая оценка угроз и защитных мер. При этом рейтинг угрозы оценивается для разных типов нарушителей, коих TARA выделяет всего три - внешний, внутренний и привилегированный внутренний.

TTP ID	Risk Score	Cyber Asset #1			Cyber Asset #2		
		External	Insider	Trusted Insider	External	Insider	Trusted Insider
T000017	4.4		4.4	4.4		4.3	4.3
T000030	4.2		4.1	4.1		4.1	4.1
T000039	3.6	3.6	3.6			3.6	
T000041	3.2	3.2	3.2		3.2	3.2	
T000053	3.0						3.0
T000064	2.9				2.9		
T000086	2.6				2.6	2.6	2.6
T000127	2.6				2.6		
T000018	2.3					2.3	2.3
T000022	2.3	2.3	2.3	2.3	2.3	2.3	2.3
T000023	2.3	2.3	2.3		2.3	2.3	
T000029	2.2	2.2	2.2		2.2	2.2	
T000048	2.0			2.0			
T000054	1.9				1.9	1.9	
T000063	1.6				1.6	1.6	
T000065	1.3	1.3					
Aggregate		14.9	22.1	12.8	21.6	30.4	18.6
Susceptibility		49.8			70.6		

Threat Assessment and Remediation Analysis (TARA)

8) TARA предлагает нейтрализовывать не все актуальные угрозы, а согласно их рейтингу. Другой предлагаемой стратегией является нейтрализация угроз, в зависимости от важности актива.

9) В первоначальной версии TARA **все защитные меры оценивались** не по трем типам эффекта (предотвращение, обнаружение и реагирование), а по 4-м - **нейтрализация угрозы, ее обнаружение, ее ограничение и восстановление после нее**. Но после появления фреймворка NIST CSF подход немного изменили.

10) Итогом моделирования угроз по TARA было составление оптимального перечня защитных мер, которые обеспечивали бы эффективную защиту от угроз/техник с минимальными затратами на внедрение и эксплуатацию.

Threat Assessment and Remediation Analysis (TARA)

- **11) Автоматизация оценки**, которая заключается в том, что все каталоги и интерфейсы для моделирования размещены в инфраструктуре MITRE, что позволяет не только обеспечить конфиденциальность проводимой оценки, но и ускорить процесс моделирования в разы по сравнению с самостоятельной разработкой инструментария для оценки.

- **12)** Интересно, что уже в 2011-м году среди угроз, которые могли быть проанализированы TARA, предусматривались не только киберугрозы, но и угрозы воздействия по техническим каналам, а также угрозы цепочке поставок.

Threat Assessment and Remediation Analysis (TARA)

13) Упомянутые в начале инструменты позволяют как создавать новые записи в каталогах, так и импортировать/экспортировать их их/во внешние системы в формате XML, искать в каталогах, а также генерировать различные отчеты. Например, вот так выглядят интерфейсы создания новой техники реализации угроз, новой защитной меры и маппинг защищаемого актива в техники реализации угроз.

14) Если первые версии TARA не фокусировались на нарушителях, то текущая версия уделяет этому вопросу немало внимания, **требуя составить профиль нарушителя**, который базируется на трех ключевых элементах - мотивация (зачем кому-то вас атаковать), цели (разведка, утечка, кража, удар по репутации и т.п.) и возможности для реализации угроз. Все эти параметры нарушителей могут меняться с течением времени, поэтому процесс составления "модели нарушителя" не статический и не одноразовый, а динамичный, требующий автоматизации.

Threat Assessment and Remediation Analysis (TARA)

15) Еще одним важным, и ранее отсутствующим элементом TARA, является **определение поверхности атаки**, которая определена как последовательность шагов нарушителя для достижения атакуемого объекта из точки входа. Понятно, что при одной точке входа и объекте атаки путей между ними может быть несколько. Также очевидно, что из одной точки входа можно попасть в множество целей, одну цель можно достичь из разных точек входа, а также что цель в случае ее компрометации может стать точкой входа для дальнейших атак. Точками входа по TARA могут быть запросы к полям баз данных, USB-порты, пользовательские учетные записи, вложения в e-mail и загружаемые из Интернет файлы, временные сетевые соединения, процессы обновления системы и т.п. В каталогах TARA многие из векторов атак, обеспечивающих переход из точки входа в точку назначения, уже прописаны и их надо просто выбирать из готового списка. Авторы TARA говорят, что более 25 векторов атак оценивать достаточно сложно.

Threat Assessment and Remediation Analysis (TARA)

Опираясь на описанные выше данные, составляется **список сценариев реализации угрозы**, которые в отличие от векторов атак и их групп, дополнены контекстом для лучшего понимания актуальных угроз.

В отличие от методики ФСТЭК TARA не требует перебора всех возможных сценариев, привязанных к техникам и тактикам.

Детали сценария	Описание
Нарушитель	Государственная хакерская группирочка
Мотивация	Военные действия
Эффект(ы)	Вывести из строя PLC. Нарушить работу системы контроля давления. Остановить работу завода
Уязвимость	ICSA-14-079-01
Точка входа	
Точка назначения	Siemens SIMATIC S7-1200 PLC
Индикаторы компрометации*	Некорректно сформированные пакеты на порт 102/TCP
Вероятность*	Низкая
Ущерб (негативный эффект)*	
Риск*	Средний
Защитные меры*	

Threat Assessment and Remediation Analysis (TARA)

- Вот такая методика была предложена MITRE десять лет назад. Во многом она похожа на то, что предложила ФСТЭК в феврале 2021, но все-таки есть и пара коренных отличий, а именно необязательность как самой методики, так и ее отдельных элементов, а также глубокая автоматизация работы на разных этапах моделирования, снижающих волюнтаризм экспертов и ускоряющих сам процесс.
- Кстати, о времени, которое требуется на моделирование угроз по методике TARA. **По оценкам ее авторов - вся процедура занимает 13 недель, то есть полный квартал с небольшим. И это при полной автоматизации.** Так что делаем выводы о том, сколько может занять моделирование угроз по текущему варианту.

Threat Assessment and Remediation Analysis (TARA)

		Рабочих недель	Рабочих часов
1	**Анализ угроз**		
1.1	Разработка модели угроз	3	120
1.2	Идентификация правдоподобных векторов атак	1	40
1.3	Оценка рисков	1	40
2	**Анализ защитных мер**		
2.1	Идентификация вероятных защитных мер	2	80
2.2	Оценка параметров защитных мер	1	40
2.3	Выбор защитных мер	1	40
3	**Управление знаниями**		
3.1	Приоритизация потребностей в информации	1	40
3.2	Идентификация и оценка внешних источников данных	2	80
3.3	Обновление каталогов	1	40
	Всего временных затрат	**13**	**520**

11. CVSS (Common Vulnerability Scoring System)

открытый стандарт для оценки степени опасности уязвимостей.

https://www.first.org/cvss/

CVSS (Common Vulnerability Scoring System)

- **CVSS разработал Национальный совет по инфраструктуре (National Infrastructure Advisory Council, NIAC) США**. Также в создании и обновлении стандарта участвовали коммерческие компании, такие как Microsoft, Cisco и другие. Поддержкой системы занимается Форум групп безопасности и реагирования на инциденты (Forum of Incident Response and Security Teams, FIRST).

- В настоящее время для оценки уязвимостей используется версия CVSS 4.0.

- **Common Vulnerability Scoring System Version 4.0**
  https://www.first.org/cvss/v4-0/
  https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf

CVSS (Common Vulnerability Scoring System)

- CVSS предлагает простой инструментарий для расчета числового показателя по десятибалльной шкале, который позволяет специалистам по безопасности оперативно принимать решение о том, как реагировать на ту или иную уязвимость.
- Чем выше значение метрики, тем более оперативная реакция требуется.

- В стандарт входят три группы метрик:
  - Базовые метрики
  - Временные метрики
  - Контекстные метрики (Метрики окружения)

Методика оценки уязвимостей по CVSS (CVSS Score)

- Согласно стандарту CVSS, уязвимости оцениваются на основании ряда метрик.
- **Можно выделить три типа метрик:**

1. **Базовые метрики**. Сюда относятся общие метрики, описывающие уязвимость и не зависящие от времени или конкретного окружения. Они делятся на две группы:
   - **Метрики эксплуатации**, описывающие, насколько уязвимость проста в эксплуатации. К этой группе относится, например, вектор атаки: одни уязвимости можно эксплуатировать через Интернет, то есть из любой точки мира с доступом к Сети, а другие требуют физического доступа к уязвимому устройству, который случайному злоумышленнику получить довольно сложно. сложность атаки, необходимость каких-либо действий со стороны пользователя и уровень привилегий, которые требуются злоумышленнику для реализации атаки.
   - **Метрики воздействия**, касающиеся последствий эксплуатации уязвимости для системы и хранящихся в ней данных. Например, может ли атакующий вывести систему из строя, получить доступ к конфиденциальным данным, модифицировать файлы и т. д.
2. **Временные метрики** описывают внешние факторы, которые могут измениться с течением времени. Например, наличие доступного эксплойта или, наоборот, патча.
3. **Метрики окружения** на основную оценку уязвимости никак не влияют, но позволяют определить ее опасность для конкретной IT-среды. В набор метрик окружения входят базовые метрики с поправкой на условия конкретной среды. Так, если для эксплуатации уязвимости в целом требуются минимальные привилегии, то в конкретной организации доступ к уязвимой системе могут иметь только администраторы. Также к метрикам окружения относятся метрики, описывающие то, насколько опасны для конкретной организации возможные последствия эксплуатации уязвимости. Например, повлияет ли на операции компании отключение сервера или у нее есть запасной сервер, на который легко переключиться в случае инцидента.

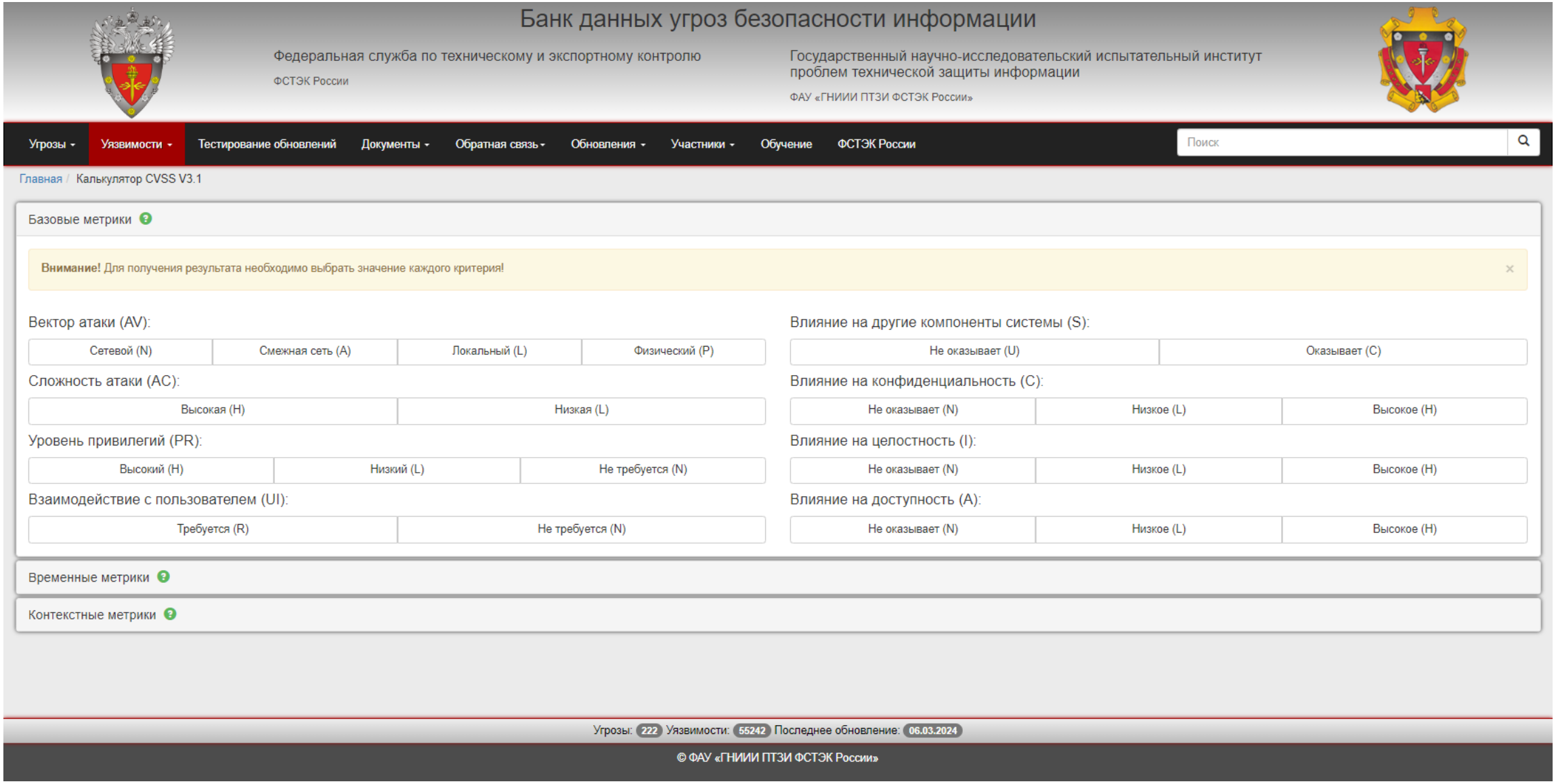
Вычисление CVSS Score

- На основании метрик с помощью набора формул вычисляется оценка CVSS Score.
- Она может принимать значение от 0 до 10, где:
  - 9,0–10,0 — критический уровень опасности;
  - 7,0–8,9 — высокий;
  - 4,0–6,9 — средний;
  - 0,1–3,9 — низкий;
  - 0 — опасность отсутствует.

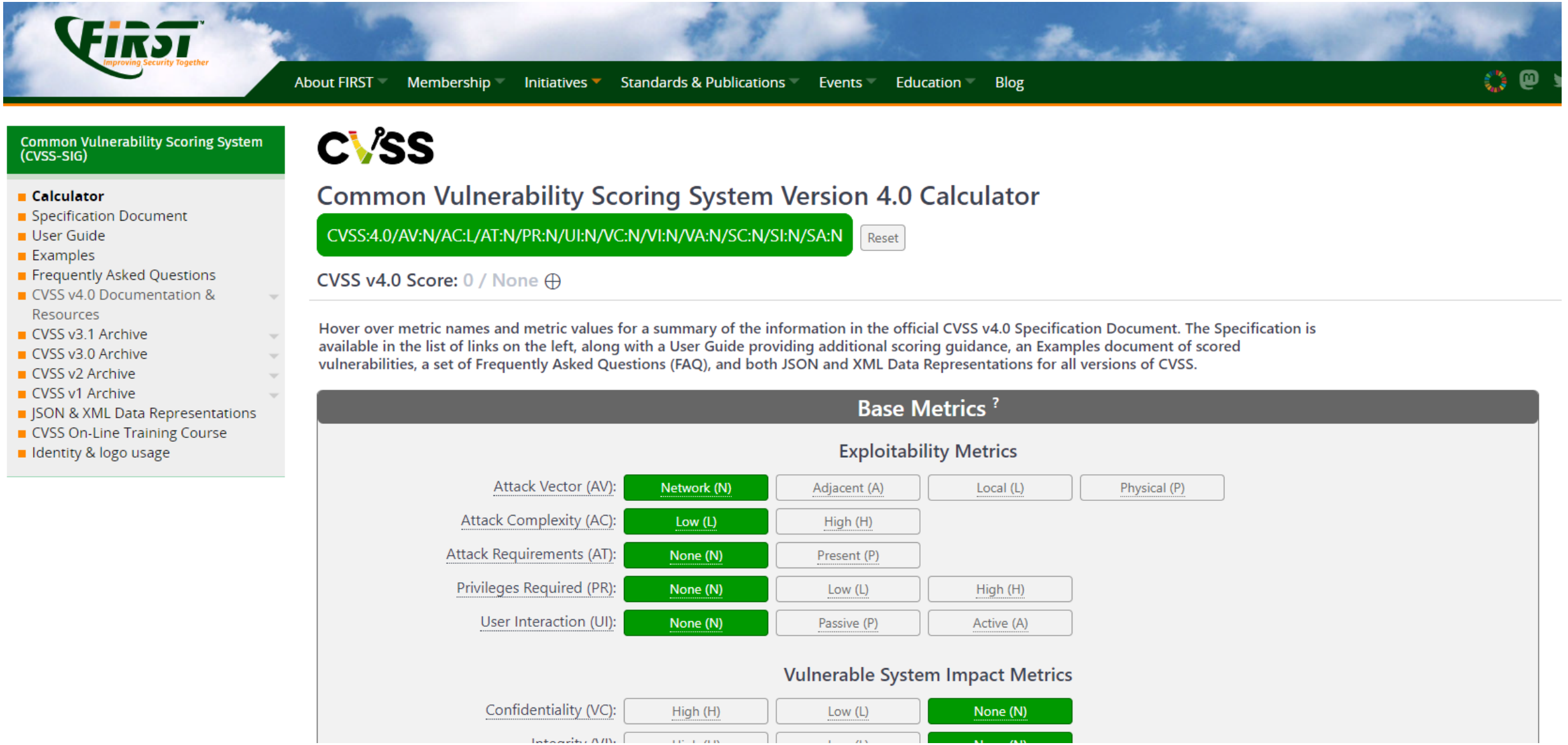
- Для упрощения расчета CVSS Score существуют онлайн-калькуляторы CVSS.

Калькулятор CVSS V 3.1

https://bdu.fstec.ru/calc31



Common Vulnerability Scoring System Version 4.0 Calculator
https://www.first.org/cvss/calculator/4.0



12. Где взять информацию о новых уязвимостях?

Классификация в области безопасности программ

Для построения оптимальных систем информационной безопасности, а также оперативного внесения изменений в их работу создано большое количество систем отслеживающих разного рода угрозы, классифицирующих, документирующих, описывающих их принцип работы и в некоторых указывающих методы защиты и борьбы с ними.

Изучение новых угроз и средств борьбы с ними очень важно для обеспечения безопасности бизнеса

Классификация в области безопасности программ

Вид	Примеры	Особенности
Классификация вредоносного программного обеспечения	**Mitre MAEC (Malware Attribute Enumeration and Characterization)** - перечень и характеристики признаков вредоносного ПО	Язык описания вредоносного ПО, учитывающий признаки поведения, тип атаки и т. п.
	Kaspersky Classification - классификация Лаборатории Касперского	Классификация вредоносного ПО по способам воздействия
	Symantec Classification - классификация фирмы Symantec	Классификация обнаруженного вредоносного ПО

Классификация в области безопасности программ

Вид	Примеры	Особенности
Реестры и классификации уязвимостей программных систем	**Mitre CVE (Common Vulnerabilities and Exposures)** - общие уязвимости и «незащищенности»	База данных известных уязви-мостей
	NVD (National Vulnerability Database) - национальная база уязвимостей США	База данных, использующая идентификаторы CVE
	OSVDB (Open Security Vulnerability Database) - база уязвимостей открытого доступа	База данных известных уязви-мостей
	US-CERT Vulnerability Notes Database - база уязвимостей	Описание уязвимостей и способов их обнаружения
	Бюллетени разработчиков: - Microsoft Bulletin ID; -Secunia ID; -VUPEN ID	Сводки найденных уязвимостей
	Таксономия Бишопа и Бейли	Устаревшая классификация уязвимостей Unix-систем

Классификация в области безопасности программ

Вид	Примеры	Особенности
Классификация угроз безопасности и компьютерных атак на ресурсы системы	**OWASP Top Ten** - 10 самых распространенных угроз для веб-приложений	Десять наиболее актуальных классов угроз, связанных с уязвимостями web-приложений за последний год
	MITRE CAPEC (Common Attack Pattern Enumeration and Classification) - перечень и классификация распространенных типов атак	Всесторонняя классификация типов атак
	Microsoft STRIDE Threat Model — модель угроз Microsoft	Описание пяти основных категорий уязвимостей
	WASC Threat Classification 2.0 — классификация угроз Консорциума безопасности web-приложений	Классификация изъянов, угроз web-безопасности, нацеленная на практическое применение

Классификация в области безопасности программ

Вид	Примеры	Особенности
Классификации дефектов, внесенных в процессе разработки	**MITRE CWE (Common Weaknesses Enumeration)** - общая классификация дефектов ПО	Система классификации «изъянов» ПО
	Fortify Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors	Классификация ошибок безопасности программного обеспечения
	CWE/SANS Top 25 Mast Dangerous Software Errors - 25 наиболее опасных ошибок в разработке ПО	25 наиболее распространенных и опасных ошибок, которые могут стать причиной уязвимости
	OWASP CLASP (OWASP Comprehensive, Lightweight, Application Security Process) - описание процесса безопасной разработки приложений	Принципы безопасности организации процесса разработки приложений

Классификация в области безопасности программ

Вид	Примеры	Особенности
Классификации дефектов, внесенных в процессе разработки	**DoD Software Fault Patterns** - образцы программных ошибок Минобороны США	Система типов дефектов ПО, ассоциированная с CWE и разработанная с целью автоматизации их выявления
	Устаревшие классификации: Устаревшие классификации: - перечни RISOS/PA - таксономия Ландвера - таксономия Аслама - таксономия Макгоу - таксономия Вебера - перечень PLOVER	Первые проекты по частичной каталогизации известных дефектов безопасности и их классификации
	MITRE Common Configuration Enumeration (CCE) - общий реестр конфигураций	Идентификация проблемных конфигураций системы, устанавливающая соответствие между различными источниками

Классификация в области безопасности программ

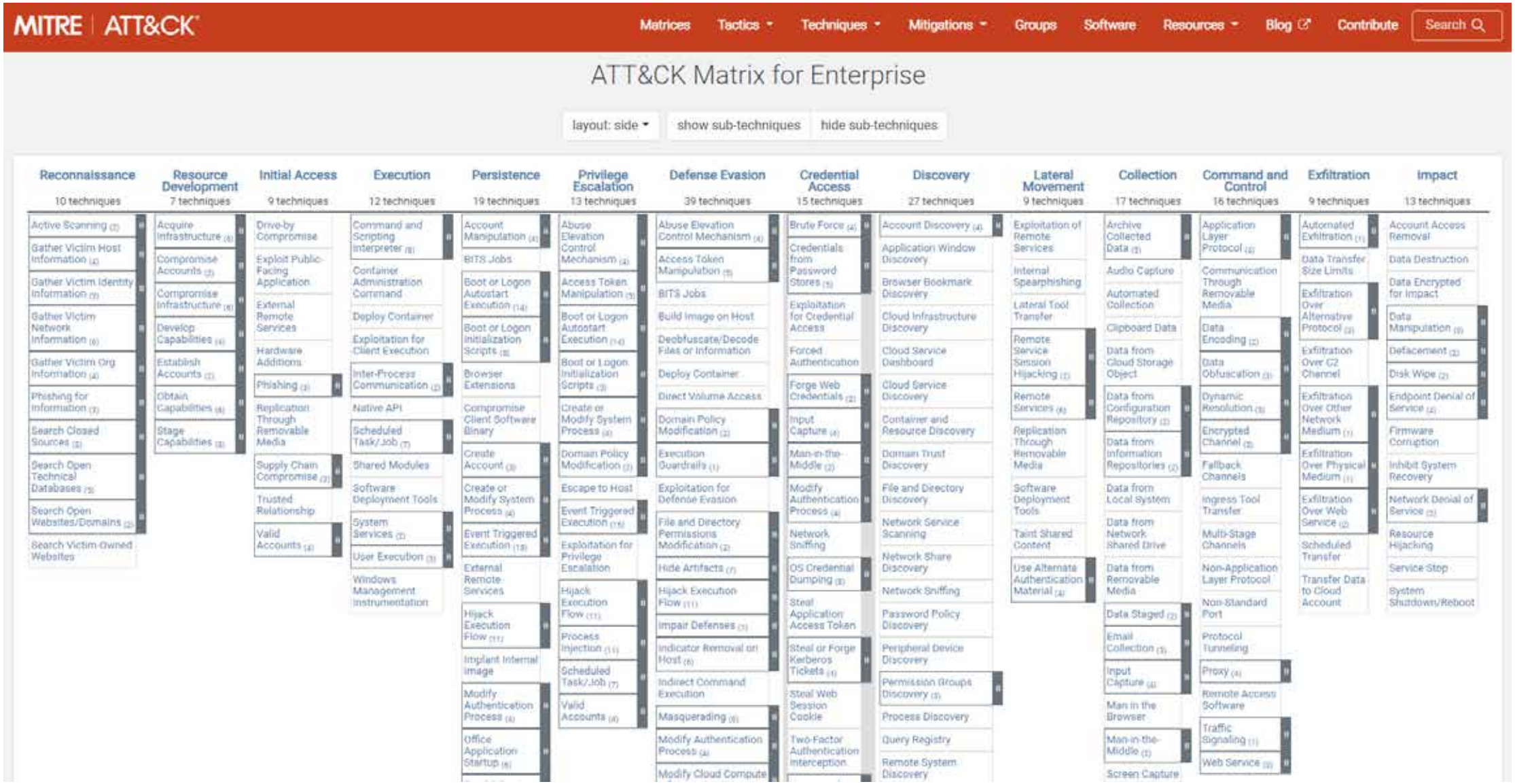
Вид	Примеры	Особенности
Классификации дефектов, внесенных в процессе внедрения и эксплуатации	**DPE (Security-Database Default Password Enumeration)** - реестр паролей но умолчанию	Основное назначение повышение эффективности аудита безопасности паролей сетевых устройств

Базы данных о выявленных уязвимостях информационных систем

Наименование БД	Ссылка
Банк данных угроз безопасности информации ФСТЭК России	http://www.bdu.fstec.ru/
Национальная база уязвимостей США, NVD (CVE)	http://nvd.nist.gov http://cve.mitre.org
База уязвимостей компании Secunia	http://secunia.com
База уязвимостей от IBM ISS (X -Force)	http://xforce.iss.net/
База уязвимостей компании Security Focus	http://www.securityfocus.com
Открытая база уязвимостей, OSV DB «Open Source Vulnerability Database»	http://osvdb.org
База эксплойтов	http://www.exploit-db.com/
Metasploit, проект, посвященный созданию средств тестирования на проникновение (эксплойтов)	http://www.metasploit.com
Сайт компании Digital Bond, занимающейся безопасностью промышленных систем	http://www.digitalbond.com
Группа реагирования на инциденты в области промышленных систем ICS - CERT «Industrial Control Systems Cyber Emergency Response Team»	http://ics-cert.us-cert.gov/
Сайт исследователя Luigi Auriemma	http://aluigi.org http://aluigi.altervista.org
Информационный портал, посвященный безопасности SCADA-систем	http://scadahacker.com
Информационный портал фирмы Positive Technologies	http://www.securitylab.ru/
Архив форумов (почтовых рассылок, «Mailing List»), посвященных ИБ	http://seclists.org
Информационный портал, посвященный вопросам ИБ, содержащий базу уязвимостей	http://www.securelist.com

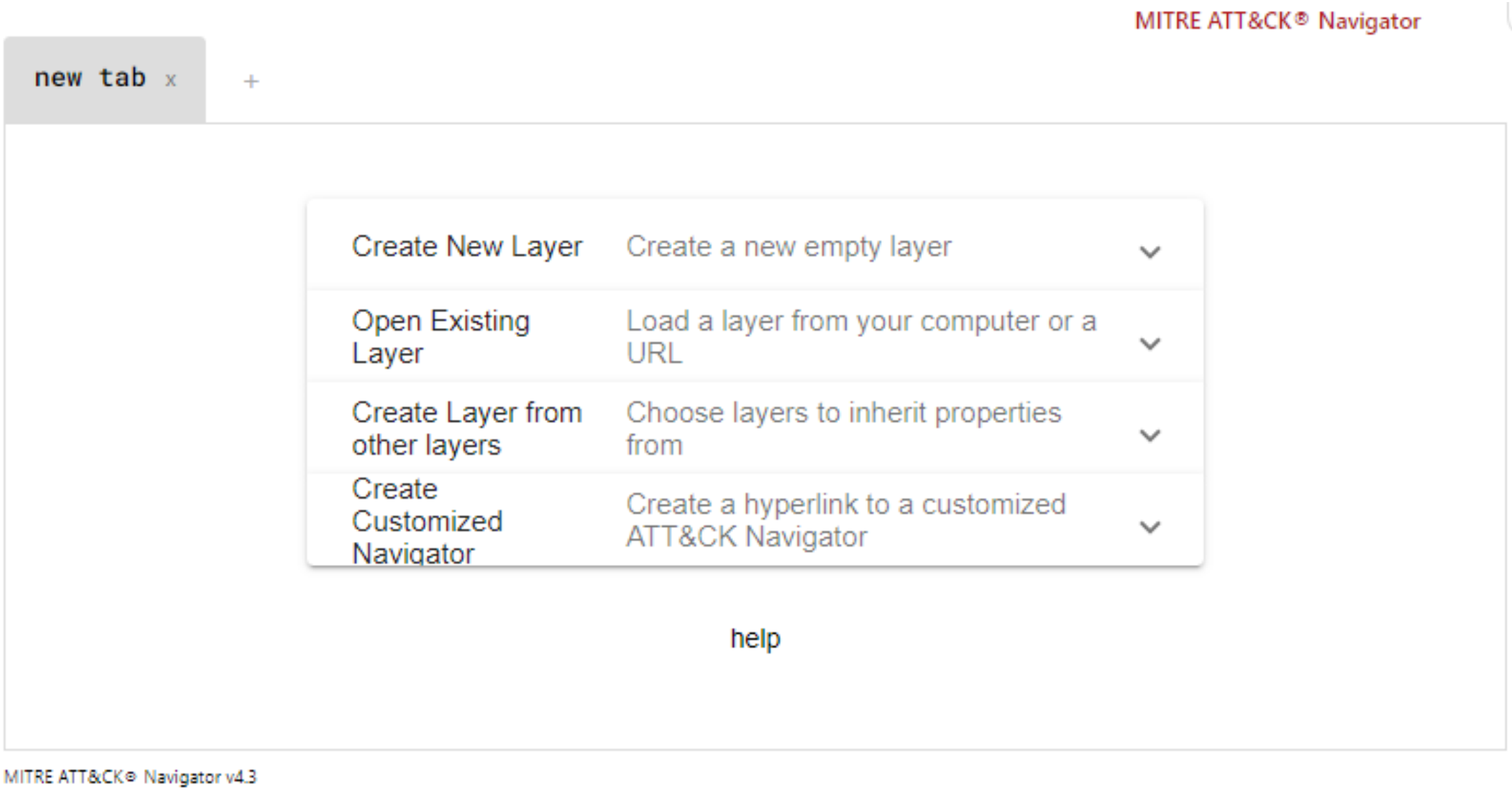
Матрица атак MITRE ATT&CK

https://attack.mitre.org



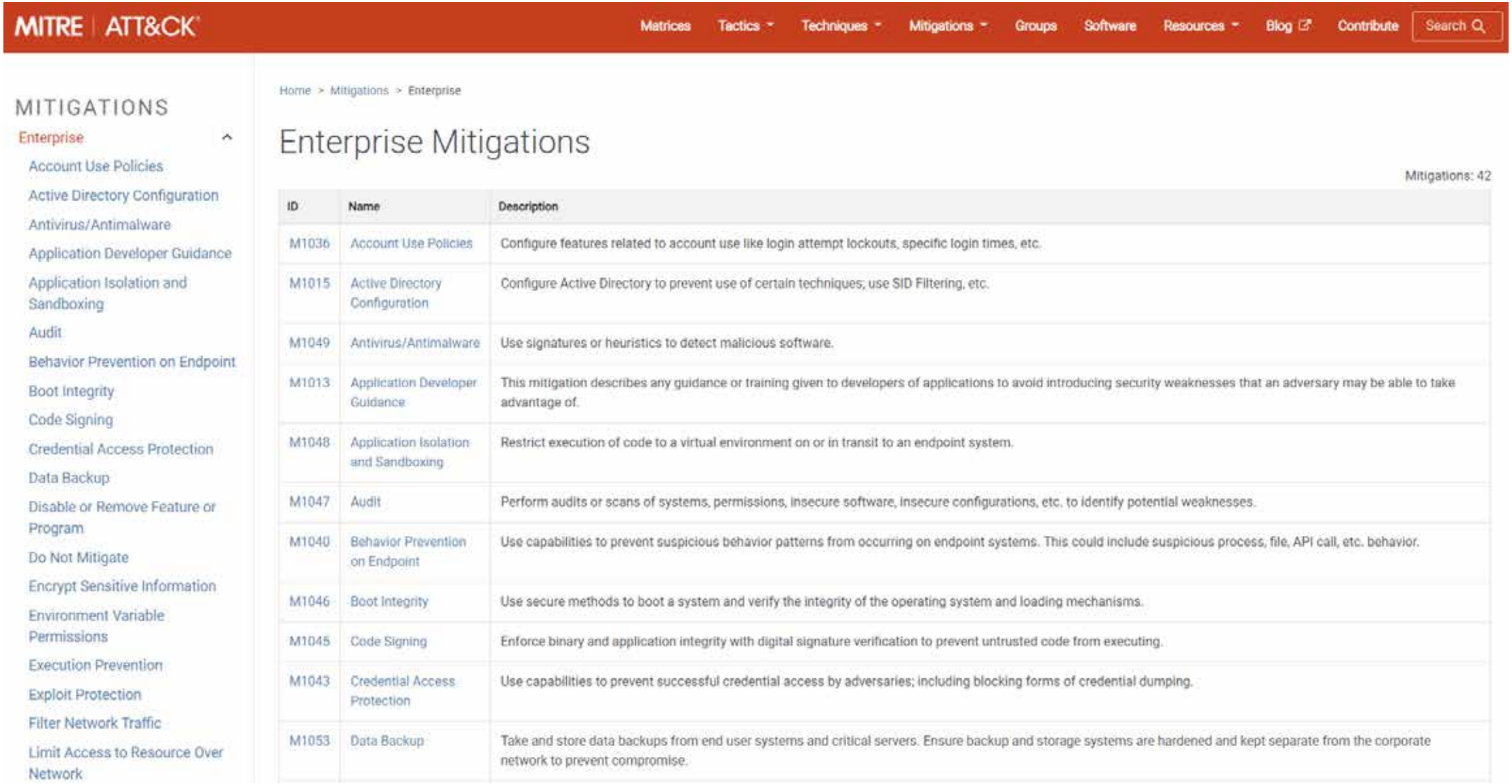
MITRE ATT&CK® Navigator **(Навигатор по матрице атак)**

https://mitre-attack.github.io/attack-navigator/



MITRE ATT&CK **Меры противодействия атакам**

https://attack.mitre.org/mitigations/enterprise/



Список уязвимостей MITRE CVE (Common Vulnerabilities and Exposures) https://cve.mitre.org

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | **Downloads** | **Data Feeds** | **Update a CVE Record** | **Request CVE IDs**

TOTAL CVE Records: 157579

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Latest CVE News

- Devolutions Added as CVE Numbering Authority (CNA)

More News >>

CVE Podcast

How the New CVE Record Format Is a Game Changer

Our new episode focuses on how the very basic legacy format of CVE Records is being transformed for the future by adding many new optional content fields, how using JSON is enabling automation for both CNA publishers and CVE content consumers, the availability of automated CNA tools for 24/7 CVE ID assignment and CVE Record publishing and updating, and more.

Listen Now >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Total CNAs: 179 | Total Countries: 30

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records

Tweets by @CVEnew

CVE
@CVEnew
CVE-2021-37436 Amazon Echo Dot devices through 2021-07-02 sometimes allow attackers, who have physical access to a device after a factory reset, to obtain sensitive information via a series of complex hardware and software attacks. NOTE: reportedly, the... cve.mitre.org/cgi-bin/cvenam...

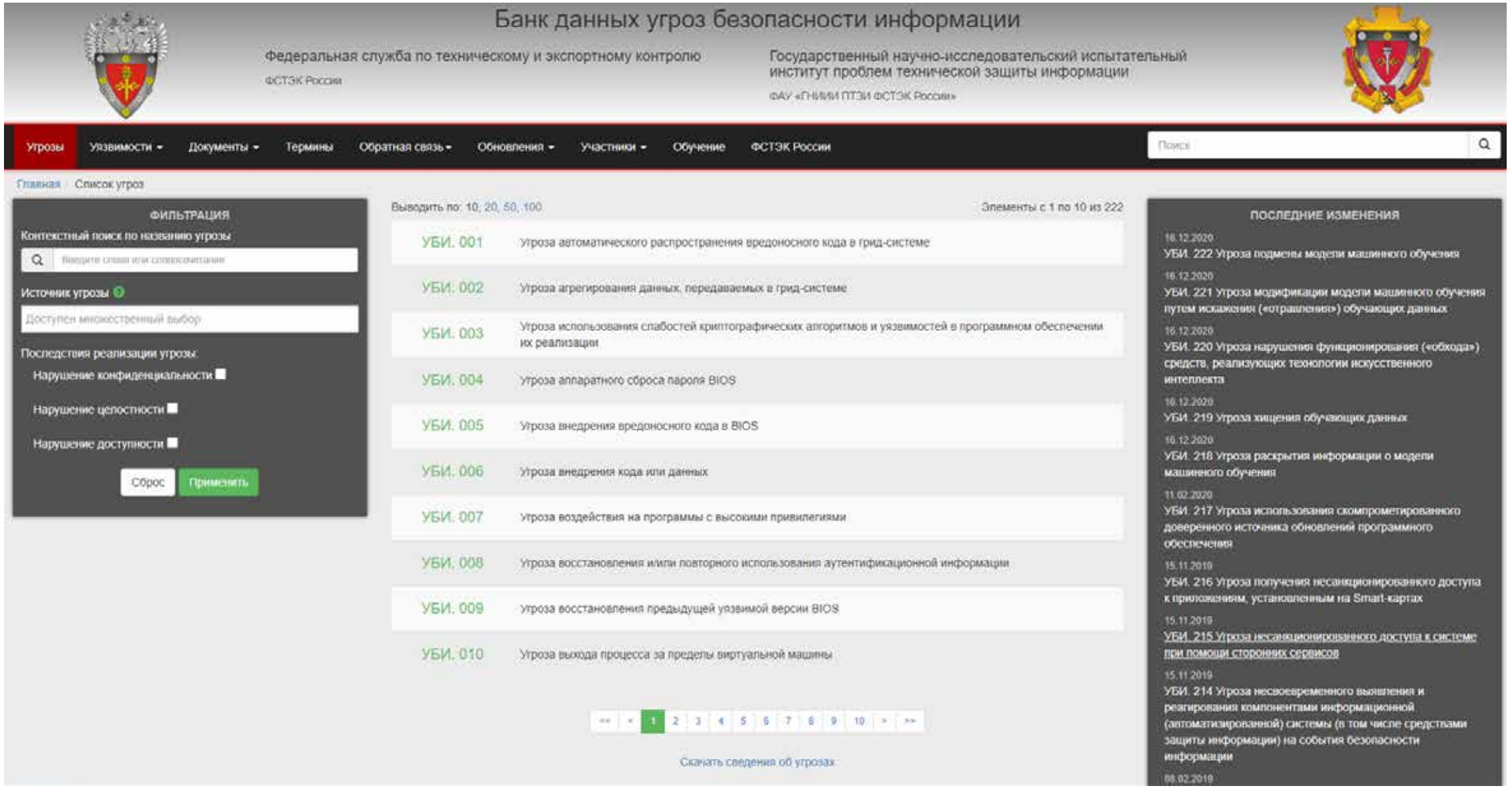
Follow @CVEnew >>

Page Last Updated or Reviewed: July 20, 2021

Site Map | Terms of Use | Privacy Policy | Contact Us | Follow CVE

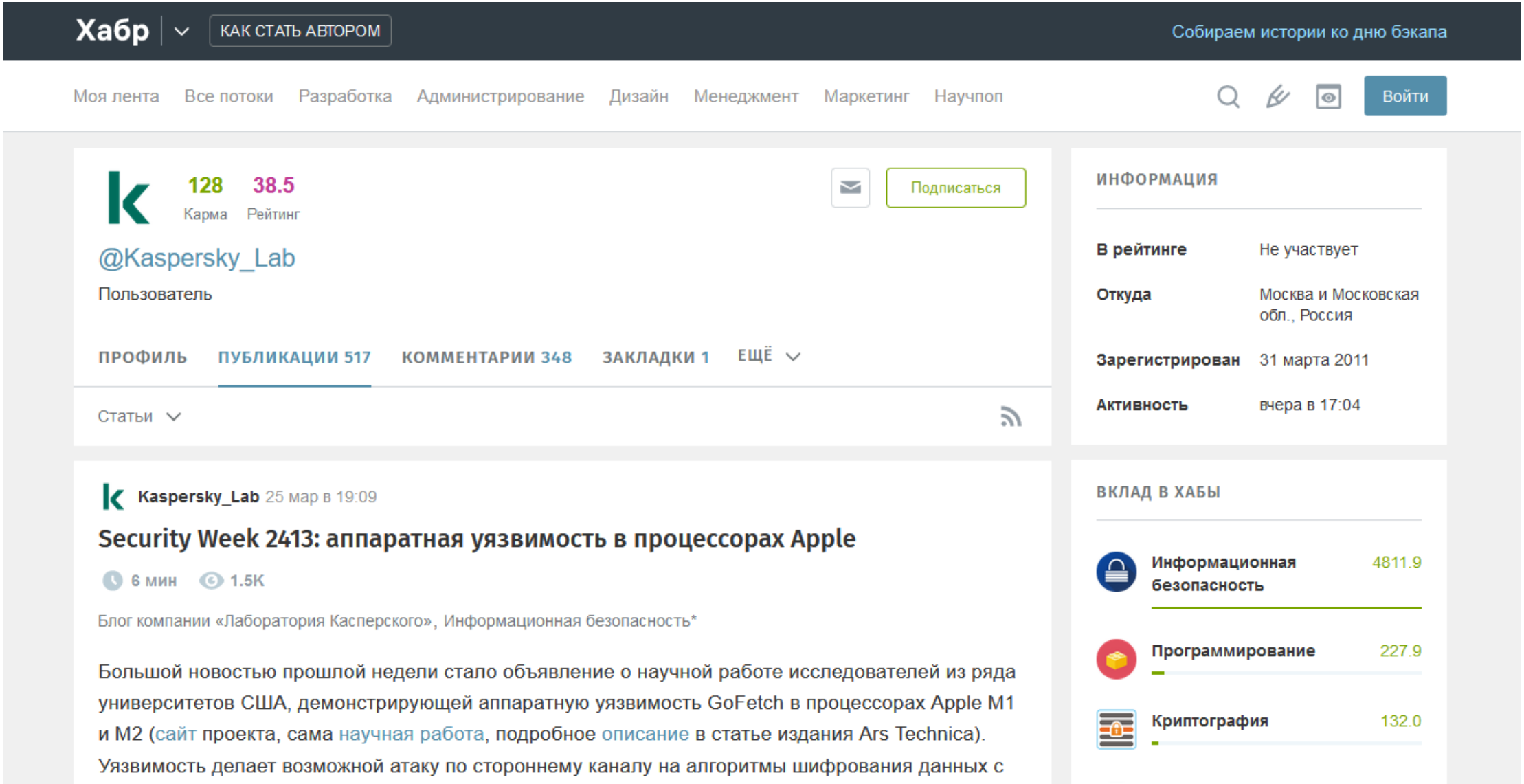
Банк данных угроз безопасности информации РФ

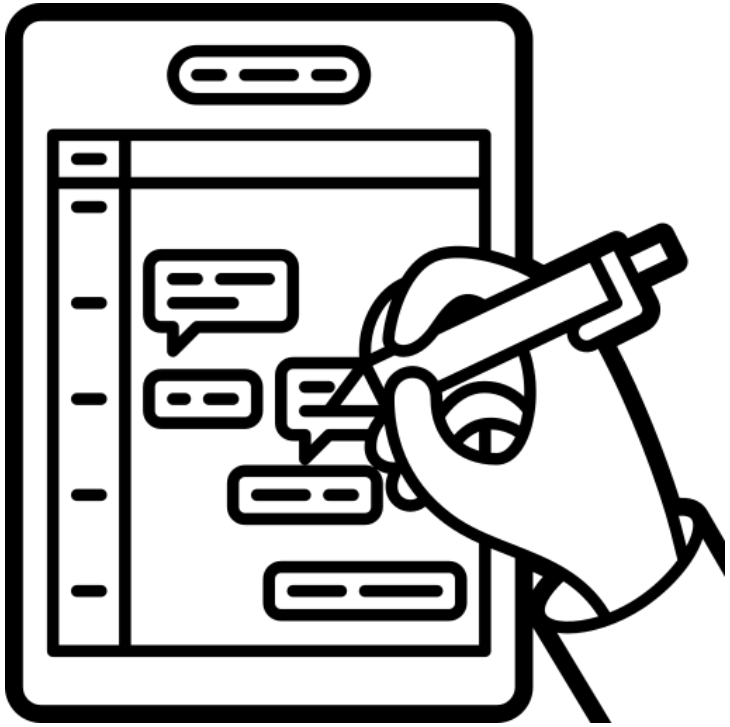
https://bdu.fstec.ru/threat



Kaspersky Security Week

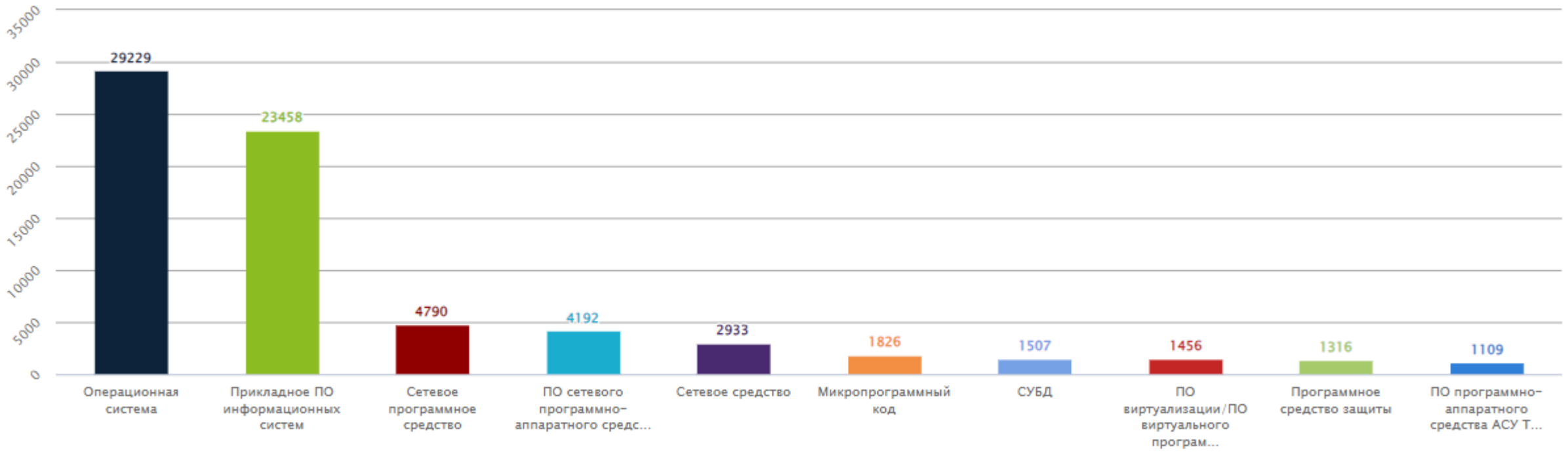
https://habr.com/ru/users/Kaspersky_Lab/posts/





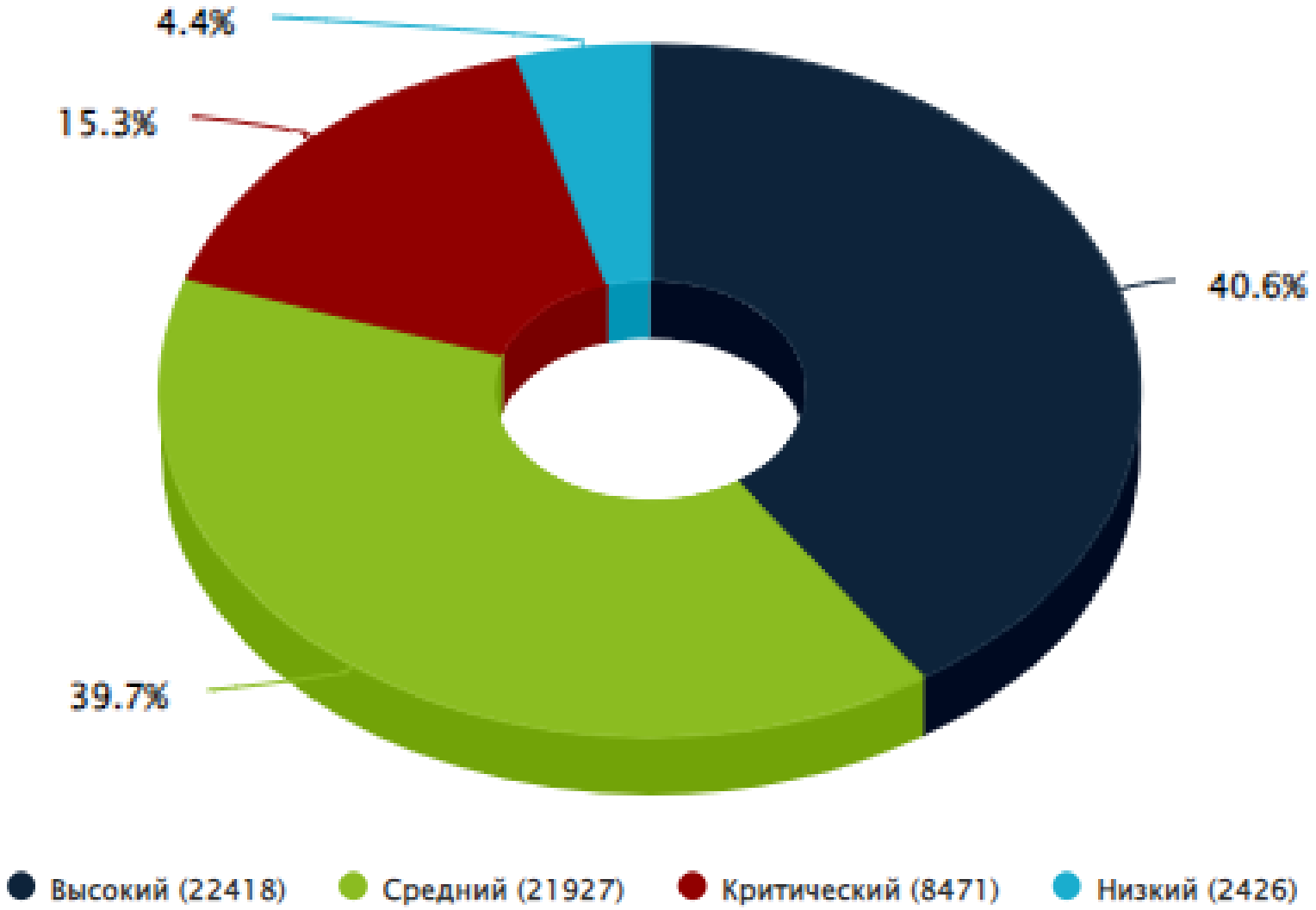
13. Статистика и инфографика по уязвимостям и угрозам

Распределение уязвимостей по типам ПО



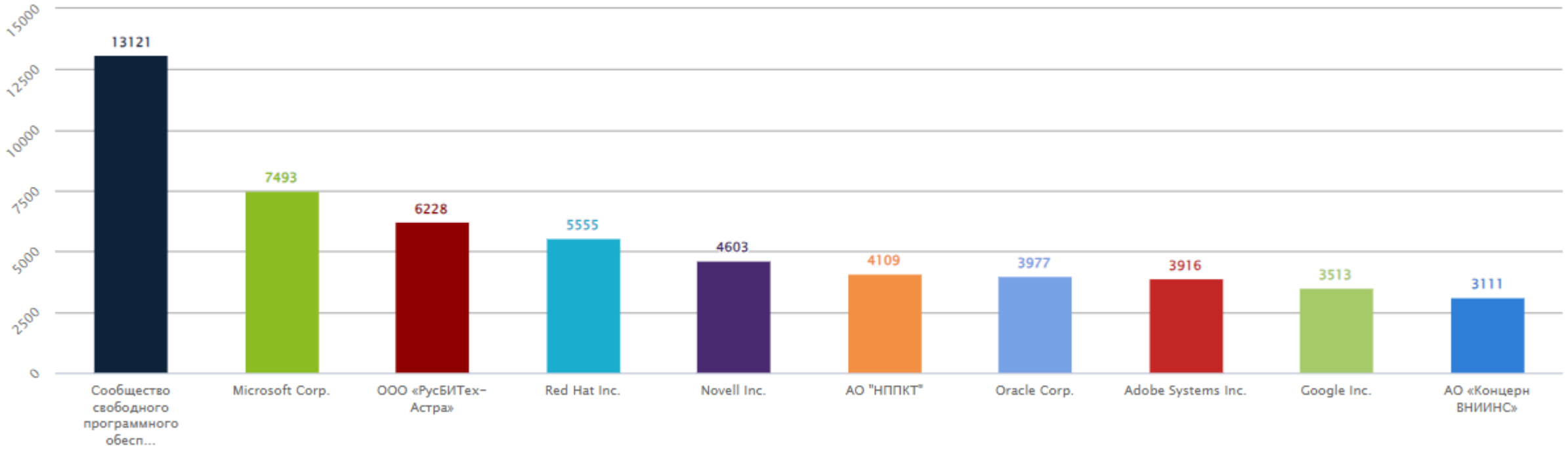
https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Распределение уязвимостей по уровням опасности



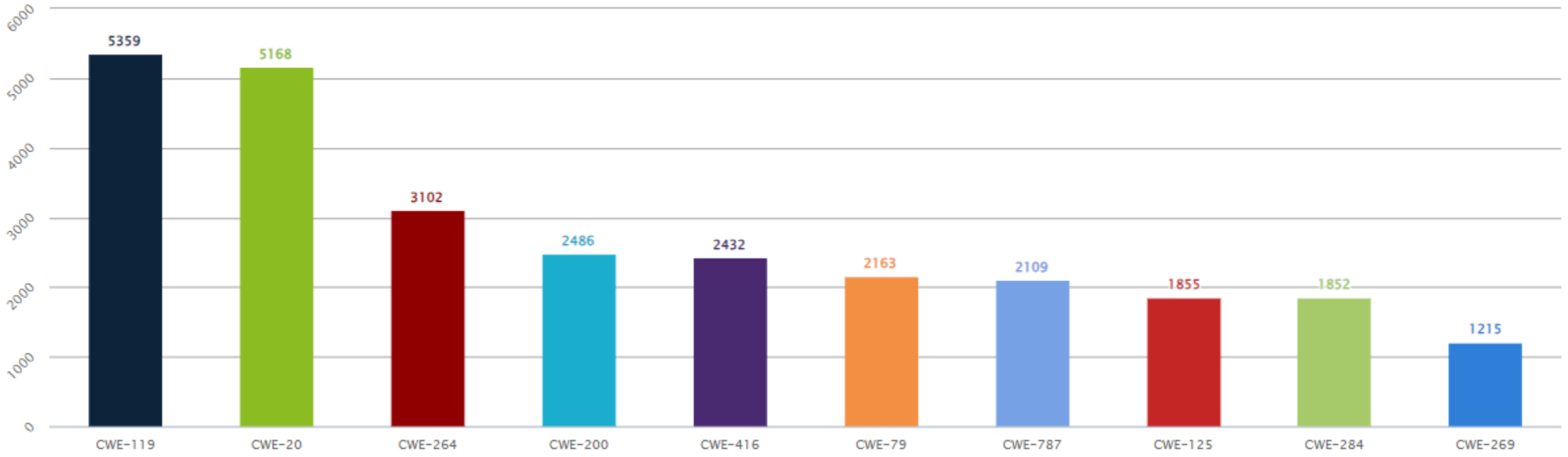
https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Количество уязвимостей в ПО различных производителей



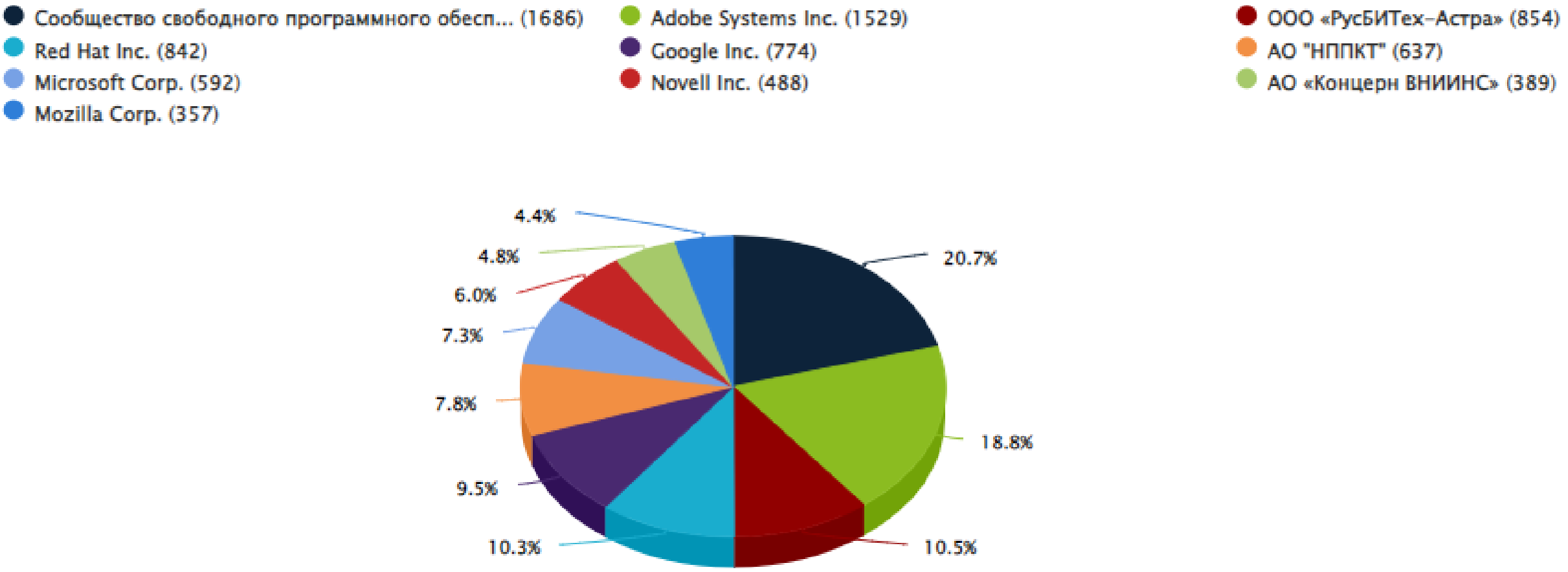
https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Распределение уязвимостей по типам ошибок



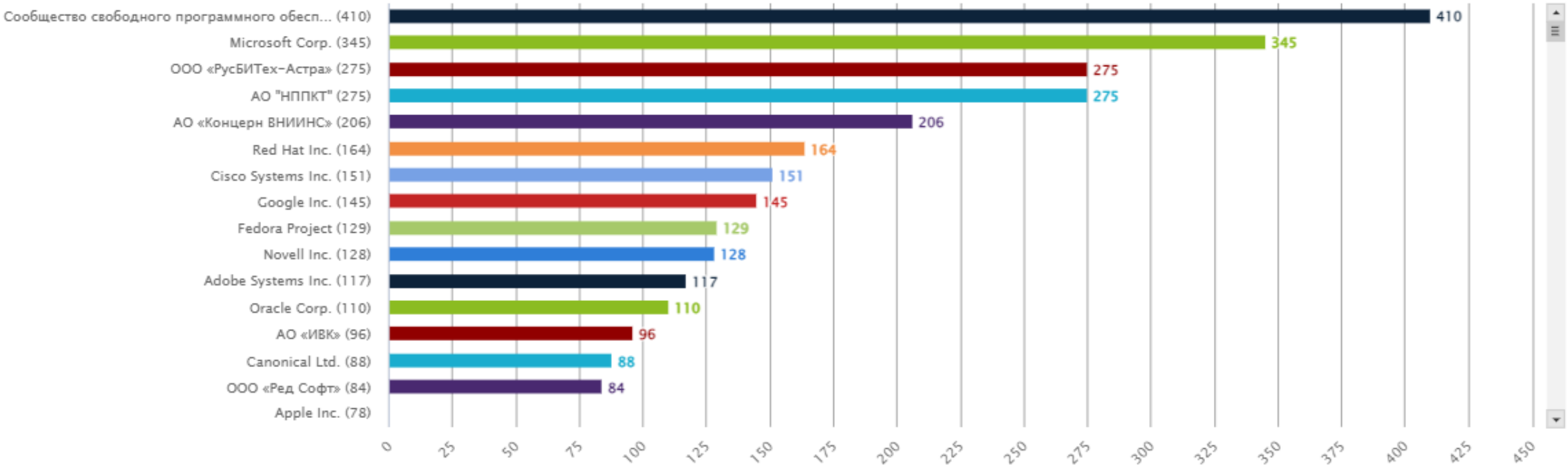
https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Количество критических уязвимостей в ПО различных производителей



https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Количество уязвимостей программного обеспечения различных производителей, связанных с инцидентами информационной безопасности



https://bdu.fstec.ru/charts - Банк данных угроз безопасности информации / Инфографика

Наиболее опасные уязвимости в соответствии с CVSS 3.0

BDU:2023-01235	Уязвимость программных платформ для разработки и управления онлайн магазинами Magento Open Source и Adobe Commerce, существующая из-за непринятия мер по защите структуры веб-страницы, позволяющая нарушителю выполнить произвольный код	11.10.2022
BDU:2023-01294	Уязвимость SCADA-системы ProMIS InSCADA, связанная с некорректной защитой исходящих сообщений об ошибках, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации	06.03.2023
BDU:2023-01735	Уязвимость платформы управления жизненным циклом моделей машинного обучения MLflow, связанная с неверным ограничением имени пути к каталогу с ограниченным доступом, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации, выполнить произвольный код или получить полный контроль над системой	24.03.2023
BDU:2023-02120	Уязвимость системы управления производственными процессами Opcenter Quality, связанная с использованием жестко закодированного криптографического ключа, позволяющая нарушителю повысить свои привилегии	13.04.2021
BDU:2023-01956	Уязвимость объекта Error.prepareStackTrace библиотеки vm2 пакетного менеджера NPM, позволяющая нарушителю выйти из изолированной программной среды и выполнить произвольный код	06.04.2023
BDU:2023-02274	Уязвимость микропрограммного обеспечения удалённого терминального блока INEA ME RTU, существующая из-за непринятия мер по нейтрализации специальных элементов, используемых в команде операционной системы, позволяющая нарушителю выполнить произвольный код	20.04.2023
BDU:2023-02379	Уязвимость микропрограммного обеспечения медицинских устройств Illumina Universal Copy Service, связанная с привязкой к открытым IP-адресам, позволяющая нарушителю прослушивать сетевой трафик, а также удаленно передавать произвольные команды	27.04.2023
BDU:2023-02459	Уязвимость микропрограммного обеспечения контроллеров Nexx Garage Door Controller (NXG-100B, NXG-200), Nexx Smart Plug (NXPG-100W), Nexx Smart Alarm (NXAL-100), связанная с использованием предустановленных учетных данных, позволяющая нарушителю получить неаутентифицированный доступ к серверу MQ Telemetry Server (MQTT)	04.04.2023
BDU:2023-02687	Уязвимость микропрограммного обеспечения маршрутизаторов InHand Networks InRouter 302 и InRouter 615, связанная с использованием недостаточно случайных значений, позволяющая нарушителю выполнить произвольный код	13.01.2023
BDU:2023-02792	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Mitsubishi Electric Corporation MELSEC iQ-F Series CPU, вызванная переполнением буфера на стеке, позволяющая нарушителю вызвать отказ в обслуживании или выполнить произвольный код	03.05.2023

https://bdu.fstec.ru/vul/danger?show=year - Наиболее опасные уязвимости в соответствии с CVSS 3.0, за год

Банк данных угроз безопасности информации / Список уязвимостей

Главная / Список уязвимостей

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО

Выберите производителя ПО

Тип ПО

Выберите тип ПО

Программное обеспечение

Выберите программное обеспечение

Аппаратная платформа

Выберите платформу

Версия ПО

Выберите версию ПО

Статус уязвимости

Выберите статус уязвимости

Доп. параметры

Диапазон дат

с

по

Уязвимости, связанные с инцидентами ИБ

Год добавления

Выберите год добавления

Класс уязвимости

Выводить по: 10, 20, 50, 100 Сортировка:

Элементы с 1 по 10 из 55242

BDU:2024-01792	Уязвимость системы непрерывной интеграции и доставки приложений (CI/CD) JetBrains TeamCity, связанная с обходом процедуры аутентификации посредством использования альтернативного пути или канала, позволяющая нарушителю выполнить произвольный код	04.03.2024
BDU:2024-01777	Уязвимость драйвера WDAC OLE DB для SQL Server операционных систем Windows, позволяющая нарушителю выполнить произвольный код	13.02.2024
BDU:2024-01780	Уязвимость драйвера WDAC OLE DB для SQL Server операционных систем Windows, позволяющая нарушителю выполнить произвольный код	13.02.2024
BDU:2024-01781	Уязвимость драйвера WDAC OLE DB для SQL Server операционных систем Windows, позволяющая нарушителю выполнить произвольный код	13.02.2024
BDU:2024-01782	Уязвимость драйвера WDAC OLE DB для SQL Server операционных систем Windows, позволяющая нарушителю выполнить произвольный код	13.02.2024
BDU:2024-01775	Уязвимость программного продукта для мониторинга устройств в реальном времени Delta Electronics InfraSuite Device Master, связанная с недостатками механизма десериализации, позволяющая нарушителю выполнить произвольный код	29.06.2023
BDU:2024-01759	Уязвимость компонента JDBC URL Handler платформы интеграции данных Apache InLong, позволяющая нарушителю выполнить произвольный код	21.05.2023
BDU:2024-01767	Уязвимость интерфейса командной строки платформы централизованного управления сетью Aruba EdgeConnect Enterprise, позволяющая нарушителю выполнить произвольный код	23.05.2023
BDU:2024-01746	Уязвимость функции sub_41D354() микропрограммного обеспечения маршрутизаторов D-Link DIR-823G, позволяющая нарушителю выполнить произвольный код или вызвать отказ в обслуживании	26.02.2024
BDU:2024-01745	Уязвимость функции sub_41D354() микропрограммного обеспечения маршрутизаторов D-Link DIR-823G, позволяющая нарушителю выполнить произвольный код или вызвать отказ в обслуживании	26.02.2024

https://bdu.fstec.ru/vul?sort=bsc

Когда так увлекся навешиванием средств защиты, что совсем позабыл про потребности бизнеса...

Защита информации

Тема: Угрозы информационной безопасности

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. М.И. Фалеев, Г.С. Черных. Угрозы национальной безопасности государства в информационной сфере https://iee.unn.ru/wp-content/uploads/sites/9/2018/02/2.Inf.ugrozy-vred.programmykomp.prestupleniya.pdf
4. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. — М.: Издательство «Аспект Пресс», 2019.— 784 с. https://mgimo.ru/upload/iblock/559/Tom%202.pdf
5. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523
6. Цирлов В. Л. Основы информационной безопасности: краткий курс / В.Л. Цирлов.– Ростов н/Д: Феникс, 2008. – 253 с. https://www.e-reading.life/bookreader.php/134422/Osnovy_informacionnoii_bezopasnosti._Kratkiii_kurs.pdf
7. Методы организации защиты информации : учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с. https://tstu.ru/book/elib/pdf/2013/martemyanov-l.pdf
8. Основы информационной безопасности критических технологий https://en.ppt-online.org/542972

Список использованных источников

9. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
10. КОНЦЕПЦИЯ национальной безопасности Республики Беларусь (Указ Президента Республики Беларусь от 09.11.2010 № 575)
https://pravo.by/document/?guid=3871&p0=P31000575
http://www.prokuratura.gov.by/ru/acts/kontseptsiya-natsionalnoy-bezopasnosti-respubliki-belarus/
11. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.)
http://www.scrf.gov.ru/security/information/document5/
http://static.kremlin.ru/media/events/files/ru/tGeA1AqAfJ4uy9jAOF4CYCpuLQw1kxdR.pdf
12. Концепция Конвенции ООН об обеспечении международной информационной безопасности
http://www.scrf.gov.ru/security/information/document112/
https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666
13. В.Н. Ясенев Конспект лекций по информационной безопасности. Нижний Новгород, 2017 – 254 с.
http://www.iee.unn.ru/wp-content/uploads/sites/9/2017/02/konspekt-lektsij-po-IB.pdf
14. PwC | Глобальное исследование «Доверие к цифровым технологиям» 2021
https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf
15. Deloitte - Управление рисками информационной безопасности
https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/3%20июня.pdf

Список использованных источников

16. **Методика оценки угроз безопасности информации ФСТЭК России**. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г.
https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021#
https://fstec.ru/component/attachments/download/2919
17. Банк данных угроз безопасности информации
http://bdu.fstec.ru
18. Обзор проекта новой методики моделирования угроз безопасности информации
https://habr.com/ru/company/acribia/blog/513178/
19. Новая методика ФСТЭК. Как теперь моделировать угрозы ИБ? (апрель 2021)
https://www.youtube.com/watch?v=rzDAJS0QVww
20. Моделирование угроз безопасности информации Подходы и инструменты
https://www.youtube.com/watch?v=CChVkqJ7p-I&list=PLQfolpjf5pQKHtNhnq-_yxFWiJLB0uRQn&index=1
21. Семинар RPPA - Методика оценки угроз безопасности информации ФСТЭК
https://www.youtube.com/watch?v=e02qqjxJwEc&list=PLQfolpjf5pQKHtNhnq-_yxFWiJLB0uRQn&index=3
22. Не методикой ФСТЭК единой или модели угроз, утвержденные государством российским
https://www.securitylab.ru/blog/personal/Business_without_danger/350967.php
23. Методика оценки угроз ФСТЭК: первая попытка применить ее на практике
https://www.securitylab.ru/blog/personal/Business_without_danger/350559.php

Список использованных источников

24. Методика оценки угроз безопасности информации – 2021
https://www.securitylab.ru/blog/personal/valerykomarov/350302.php
25. Краткий обзор новой методики оценки угроз ФСТЭК
https://www.securitylab.ru/blog/personal/Business_without_danger/350381.php
26. Простыми словами о новом проекте методики моделирования угроз безопасности информации ФСТЭК
https://www.securitylab.ru/blog/company/axxtel/348258.php
27. Магия моделирования угроз по ФСТЭК
https://www.securitylab.ru/blog/personal/Business_without_danger/350797.php
28. Моделирование нарушителей по методике ФСТЭК: теория и реальность
https://www.securitylab.ru/blog/personal/Business_without_danger/350598.php
29. От техник и тактик угроз к мерам обнаружения и защиты. Как сопоставить первое со вторым?
https://www.securitylab.ru/blog/personal/Business_without_danger/350864.php
30. Бизнес без опасности
https://www.securitylab.ru/blog/personal/Business_without_danger/
31. MITRE
https://www.mitre.org
32. Список уязвимостей CVE (Common Vulnerabilities and Exposures)
http://cve.mitre.org
33. Adversarial ML Threat Matrix
https://github.com/mitre/advmlthreatmatrix

Список использованных источников

34. MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge)
https://attack.mitre.org
35. Матрица ATT&CK. Как устроен язык описания угроз и как его используют
https://xakep.ru/2021/03/17/mitre-att-ck/
36. TARA - методология моделирования угроз и защитных мер от MITRE
https://www.securitylab.ru/blog/personal/Business_without_danger/351001.php
37. Threat Assessment and Remediation Analysis (TARA)
https://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-and-remediation-analysis.pdf
38. MITRE-мания. Руководство по анализу результатов тестирований ATT&CK
https://blog.tiger-optics.ru/2021/04/mitre-engenuity/
39. Систематика уязвимостей и дефектов безопасности программных ресурсов / Защита информации. INSIDE № 3'2013
https://npo-echelon.ru/doc/is_taxonomy.pdf
40. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности
https://cyberrus.com/wp-content/uploads/2021/04/68-83-343-21_7.-Garbuk.pdf
41. MITRE ATT&CK® Navigator (Навигатор по матрице атак)
https://mitre-attack.github.io/attack-navigator/
42. MITRE ATT&CK Меры противодействия атакам
https://attack.mitre.org/mitigations/enterprise/

Список использованных источников

43. Банк данных угроз безопасности информации РФ
https://bdu.fstec.ru/threat

44. Kaspersky Security Week
https://habr.com/ru/users/Kaspersky_Lab/posts/

45. Alert (AA21-209A) Top Routinely Exploited Vulnerabilities.
https://us-cert.cisa.gov/ncas/alerts/aa21-209a

46. Австралия, США и Великобритания представили список самых популярных уязвимостей
https://www.securitylab.ru/news/522876.php

47. **СТБ 34.101.72-2018** Информационные технологии. Методы и средства безопасности. Технические средства обработки информации. **Классификация угроз безопасности, связанных с наличием закладных устройств и недекларированных функций**

48. Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя (2017). http://www.rv-lab.ru/it/is/Амелин%20Р.В.%20Информационная%20безопасность.%20Лекция%206.%20Угрозы%20информационной%20безопасности.pdf

49. Как ранжировать уязвимости по уровню опасности (02 февраля 2024 - 10:32)
https://www.anti-malware.ru/practice/methods/How-to-rank-vulnerabilities-by-severity-level